Cityroots
Inc.
Technology Consulting Group

7112 Aztec Way
Bakersfield, Ca 93308
Office: (661) 703-9363
Fax: (661) 589-8849
www.cityroots.com

FEDERAL ACQUISITION SERVICES
INFORMATION TECHNOLOGY SCHEDULE PRICELIST
GENERAL PURPOSE COMMERCIAL INFORMATION TECHNOLOGY EQUIPMENT, SOFTWARE AND SERVICES

Special Item No. 132-3	Leasing Of Product
Special Item No. 132-32	Term Software Licenses
Special Item No. 132-34	Maintenance of Software
Special Item No. 132-50	Training Courses for Information Technology Equipment And Software
Special Item No. 132-51	Information Technology Professional Services

SIN 132-3 – Leasing Of Product

SIN 132-32 – Term Software Licenses

FSC Class 7030 .... Information Technology Software

Microcomputers
Application Software
Utility Software

SIN 132-34 – Maintenance of Software

SIN 132-50 – Training Courses For Information Technology Equipment and Software (FPDS Code U012)

SIN 132-51 – Information Technology (IT) Professional Services

FPDS Code D301	IT Facility Operation and Maintenance
FPDS Code D306	IT Systems Analysis Services
FPDS Code D310	IT Backup and Security Services
FPDS Code D316	IT Network Management Services
FPDS Code D399	Other Information Technology Services, Not Elsewhere Classified

Contract Number: **GS-35F-0180S**

Period Covered by Contract: **January 19, 2006** thru **January 19, 2011**

General Services Administration
Federal Supply Service

Pricelist current as of: **June 16, 2008**

Products and ordering information in this Authorized FSS Information Technology Schedule Pricelist are also available on the GSA Advantage! System. Agencies can browse GSA Advantage! by accessing the Federal Supply Service's Home Page via the Internet at http://www.fss.gsa.gov/.

TABLE OF CONTENTS

Cityroots Inc.
Technology Consulting Group

7112 Aztec Way
Bakersfield, Ca 93308
Office: (661) 703-9363
Fax: (661) 589-8849
www.cityroots.com

INFORMATION FOR ORDERING ACTIVITIES
APPLICABLE TO ALL SPECIAL ITEM NUMBERS

SPECIAL NOTICE TO AGENCIES: Small Business Participation

SBA strongly supports the participation of small business concerns in the Federal Supply Schedules Program. To enhance Small Business Participation SBA policy allows agencies to include in their procurement base and goals, the dollar value of orders expected to be placed against the Federal Supply Schedules, and to report accomplishments against these goals.

For orders exceeding the micropurchase threshold, FAR 8.404 requires agencies to consider the catalogs/pricelists of at least three schedule contractors or consider reasonably available information by using the GSA Advantage!™ on-line shopping service (www.fss.gsa.gov). The catalogs/pricelists, GSA Advantage!™ and the Federal Supply Service Home Page (www.fss.gsa.gov) contains information on a broad array of products and services offered by small business concerns.

This information should be used as a tool to assist ordering activities in meeting or exceeding established small business goals. It should also be used as a tool to assist in including small, small disadvantaged, and women-owned small businesses among those considered when selecting pricelists for a best value determination.

For orders exceeding the micropurchase threshold, customers are to give preference to small business concerns when two or more items at the same delivered price will satisfy their requirement.

1. Geographic Scope of Contract:

Domestic delivery is delivery within the 48 contiguous states, Alaska, Hawaii, Puerto Rico, Washington, DC, and U.S. Territories. Domestic delivery also includes a port or consolidation point, within the aforementioned areas, for orders received from overseas activities.

Overseas delivery is delivery to points outside of the 48 contiguous states, Washington, DC, Alaska, Hawaii, Puerto Rico, and U.S. Territories.

Offerors are requested to check one of the following boxes:

☐ The Geographic Scope of Contract will be domestic and overseas delivery.
☐ The Geographic Scope of Contract will be overseas delivery only.
☒ The Geographic Scope of Contract will be domestic delivery only.

For Special Item Number 132-53 Wireless Services ONLY, if awarded, list the limited geographic coverage area:

Not Applicable

2. Contractor's Ordering Address and Payment Information:

Ordering & Payment Address
Cityroots, Inc.
7112 Aztec Way
Bakersfield, CA 93308

Contractors are required to accept credit cards for payments equal to or less than the micro-purchase threshold for oral or written delivery orders. Credit cards will be acceptable for payment above the micro-purchase threshold. In addition, bank account information for wire transfer payments will be shown on the invoice.

The following telephone number(s) can be used by ordering activities to obtain technical and/or ordering assistance:

Ordering & Technical Assistance

Deborah Ramirez-Tinoco
Telephone Number: (661) 588-0639
Fax Number: (661) 589-8849
E-mail: deb@cityroots.com

Darren Newell
Telephone Number: (925) 672-2008
Fax Number: (661) 589-8849
E-mail: dnewell@cityroots.com

3. Liability For Injury Or Damage

The Contractor shall not be liable for any injury to ordering activity personnel or damage to ordering activity property arising from the use of equipment maintained by the Contractor, unless such injury or damage is due to the fault or negligence of the Contractor.

4. Statistical Data for Government Ordering Office Completion of Standard Form 279:

Block 9: G. Order/Modification Under Federal Schedule
Block 16: Data Universal Numbering System (DUNS) Number: 04-363-4224
Block 30: Type of Contractor – B. Other Small Business

A. Small Disadvantaged Business
B. Other Small Business
C. Large Business
D. Other Nonprofit Organization
L. Foreign Contractor

Block 31: Woman-Owned Small Business – Yes
Block 36: Contractor's Taxpayer Identification Number (TIN): 77-0565398

4a. CAGE Code: 3RHU8

4b. Contractor has registered with the Central Contractor Registration Database.

5. FOB Destination – Not Applicable

6. DELIVERY SCHEDULE

a. TIME OF DELIVERY: The Contractor shall deliver to destination within the number of calendar days after receipt of order (ARO), as set forth below:

SPECIAL ITEM NUMBER	DELIVERY TIME (Days ARO)
132-3; 132-32; 132-34	30 Days
132-50; 132-51	30 Days

b. URGENT REQUIREMENTS: When the Federal Supply Schedule contract delivery period does not meet the bona fide urgent delivery requirements of an ordering activity, ordering activities are encouraged, if time permits, to contact the Contractor for the purpose of obtaining accelerated delivery. The Contractor shall reply to the inquiry within 3 workdays after receipt. (Telephonic replies shall be confirmed by the Contractor in writing.) If the Contractor offers an accelerated delivery time acceptable to the ordering activity, any order(s) placed pursuant to the agreed upon accelerated delivery time frame shall be delivered within this shorter delivery time and in accordance with all other terms and conditions of the contract.

7. Discounts: Prices shown are NET Prices; Basic Discounts have been deducted.

a. Prompt Payment: 0 % for 0 days from receipt of invoice or date of acceptance, whichever is later

b. Quantity

c. Dollar Volume

d. Government Educational Institutions

e. Other – None

8. Trade Agreements Act of 1979, as amended:

All items are U.S. made end products, designated country end products, Caribbean Basin country end products, Canadian end products, or Mexican end products as defined in the Trade Agreements Act of 1979, as amended.

9. Statement Concerning Availability of Export Packing:

10. Small Requirements: The minimum dollar value of orders to be issued is $ 100.00 .

11. Maximum Order (All dollar amounts are exclusive of any discount for prompt payment.)

a. The Maximum Order value for the following Special Item Numbers (SINs) is $500,000:

Special Item Number 132-32 - Term Software Licenses
Special Item Number 132-34 – Maintenance of Software
Special Item Number 132-51 - Information Technology (IT) Professional Services

b. The Maximum Order value for the following Special Item Numbers (SINs) is $25,000:

Special Item Number 132-50 - Training Courses

12. USE OF FEDERAL SUPPLY SERVICE INFORMATION TECHNOLOGY SCHEDULE CONTRACTS. In accordance with FAR 8.404:

[**NOTE**: Special ordering procedures have been established for Special Item Numbers (SINs) 132-51 IT Professional Services and 132-52 EC Services; refer to the terms and conditions for those SINs.]

Orders placed pursuant to a Multiple Award Schedule (MAS), using the procedures in FAR 8.404, are considered to be issued pursuant to full and open competition. Therefore, when placing orders under Federal Supply Schedules, ordering activities need not seek further competition, synopsize the requirement, make a separate determination of fair and reasonable pricing, or consider small business set-asides in accordance with subpart 19.5. GSA has already determined the prices of items under schedule contracts to be fair and reasonable. By placing an order against a schedule using the procedures outlined below, the ordering activity has concluded that the order represents the best value and results in the lowest overall cost alternative (considering price, special features, administrative costs, etc.) to meet the ordering activity's needs.

a. Orders placed at or below the micro-purchase threshold. Ordering activities can place orders at or below the micro-purchase threshold with any Federal Supply Schedule Contractor.

b. Orders exceeding the micro-purchase threshold but not exceeding the maximum order threshold. Orders should be placed with the Schedule Contractor that can provide the supply or service that represents the best value. Before placing an order, ordering activities should consider reasonably available information about the supply or service offered under MAS contracts by using the "GSA Advantage!" on-line shopping service, or by reviewing the catalogs/pricelists of at least three Schedule Contractors and selecting the delivery and other options available under the schedule that meets the ordering activity's needs. In selecting the supply or service representing the best value, the ordering activity may consider--

(1) Special features of the supply or service that are required in effective program performance and that are not provided by a comparable supply or service;

(2) Trade-in considerations;

(3) Probable life of the item selected as compared with that of a comparable item;

(4) Warranty considerations;

(5) Maintenance availability;

(6) Past performance; and

(7) Environmental and energy efficiency considerations.

c. Orders exceeding the maximum order threshold. Each schedule contract has an established maximum order threshold. This threshold represents the point where it is advantageous for the ordering activity to seek a price reduction. In addition to following the procedures in paragraph b, above, and before placing an order that exceeds the maximum order threshold, ordering activities shall--

Review additional Schedule Contractors'

(1) Catalogs/pricelists or use the "GSA Advantage!" on-line shopping service;

(2) Based upon the initial evaluation, generally seek price reductions from the Schedule Contractor(s) appearing to provide the best value (considering price and other factors); and

(3) After price reductions have been sought, place the order with the Schedule Contractor that provides the best value and results in the lowest overall cost alternative. If further price reductions are not offered, an order may still be placed, if the ordering activity determines that it is appropriate.

NOTE: For orders exceeding the maximum order threshold, the Contractor may:

(1) Offer a new lower price for this requirement (the Price Reductions clause is not applicable to orders placed over the maximum order in FAR 52.216-19 Order Limitations);

(2) Offer the lowest price available under the contract; or

(3) Decline the order (orders must be returned in accordance with FAR 52.216-19).

d. Blanket purchase agreements (BPAs). The establishment of Federal Supply Schedule BPAs is permitted when following the ordering procedures in FAR 8.404. All schedule contracts contain BPA provisions. Ordering activities may use BPAs to establish accounts with Contractors to fill recurring requirements. BPAs should address the frequency of ordering and invoicing, discounts, and delivery locations and times.

e. Price reductions. In addition to the circumstances outlined in paragraph c, above, there may be instances when ordering activities will find it advantageous to request a price reduction. For example, when the ordering activity finds a schedule supply or service elsewhere at a lower price or when a BPA is being established to fill recurring requirements, requesting a price reduction could be advantageous. The potential volume of orders under these agreements, regardless of the size of the individual order, may offer the ordering activity the opportunity to secure greater discounts. Schedule Contractors are not required to pass on to all schedule users a price reduction extended only to an individual ordering activity for a specific order.

f. Small business. For orders exceeding the micro-purchase threshold, ordering activities should give preference to the items of small business concerns when two or more items at the same delivered price will satisfy the requirement.

g. Documentation. Orders should be documented, at a minimum, by identifying the Contractor the item was purchased from, the item purchased, and the amount paid. If an ordering activity requirement, in excess of the micro-purchase threshold, is defined so as to require a particular brand name, product, or feature of a product peculiar to one manufacturer, thereby precluding consideration of a product manufactured by another company, the ordering activity shall include an explanation in the file as to why the particular brand name, product, or feature is essential to satisfy the ordering activity's needs.

13. FEDERAL INFORMATION TECHNOLOGY/TELECOMMUNICATION STANDARDS REQUIREMENTS: ordering activities acquiring products from this Schedule must comply with the provisions of the Federal Standards Program, as appropriate (reference: NIST Federal Standards Index). Inquiries to determine whether or not specific products listed herein comply with Federal Information Processing Standards (FIPS) or Federal Telecommunication Standards (FED-STDS), which are cited by ordering activities, shall be responded to promptly by the Contractor.

13.1 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATIONS (FIPS PUBS): Information Technology products under this Schedule that do not conform to Federal Information Processing Standards (FIPS) should not be acquired unless a waiver has been granted in accordance with the applicable "FIPS Publication." Federal Information Processing Standards Publications (FIPS PUBS) are issued by the U.S. Department of Commerce, National Institute of Standards and Technology (NIST), pursuant to National Security Act. Information concerning their availability and applicability should be obtained from the National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, Virginia 22161. FIPS PUBS include voluntary standards when these are adopted for Federal use. Individual orders for FIPS PUBS should be referred to the NTIS Sales Office, and orders for subscription service should be referred to the NTIS Subscription Officer, both at the above address, or telephone number (703) 487-4650.

13.2 FEDERAL TELECOMMUNICATION STANDARDS (FED-STDS): Telecommunication products under this Schedule that do not conform to Federal Telecommunication Standards (FED-STDS) should not be acquired unless a waiver has been granted in accordance with the applicable "FED-STD." Federal Telecommunication Standards are issued by the U.S. Department of Commerce, National Institute of Standards and Technology (NIST), pursuant to National Security Act. Ordering information and information concerning the availability of FED-STDS should be obtained from the GSA, Federal Supply Service, Specification Section, 470 East L'Enfant Plaza, Suite 8100, SW, Washington, DC 20407, telephone number (202) 619-8925. Please include a self-addressed mailing label when requesting information by mail. Information concerning their applicability can be obtained by writing or calling the U.S. Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD 20899, telephone number (301) 975-2833.

14. CONTRACTOR TASKS / SPECIAL REQUIREMENTS (C-FSS-370) (NOV 2001)

a. Security Clearances: The Contractor may be required to obtain/possess varying levels of security clearances in the performance of orders issued under this contract. All costs associated with obtaining/possessing such security clearances should be factored into the price offered under the Multiple Award Schedule.

b. Travel: The Contractor may be required to travel in performance of orders issued under this contract. Allowable travel and per diem charges are governed by Pub .L. 99-234 and FAR Part 31, and are reimbursable by the ordering agency or can be priced as a fixed price item on orders placed under the Multiple Award Schedule. The Industrial Funding Fee does NOT apply to travel and per diem charges.

c. Certifications, Licenses and Accreditations: As a commercial practice, the Contractor may be required to obtain/possess any variety of certifications, licenses and accreditations for specific FSC/service code classifications offered. All costs associated with obtaining/ possessing such certifications, licenses and accreditations should be factored into the price offered under the Multiple Award Schedule program.

d. Insurance: As a commercial practice, the Contractor may be required to obtain/possess insurance coverage for specific FSC/service code classifications offered. All costs associated with obtaining/possessing such insurance should be factored into the price offered under the Multiple Award Schedule program.

e. Personnel: The Contractor may be required to provide key personnel, resumes or skill category descriptions in the performance of orders issued under this contract. Ordering activities may require agency approval of additions or replacements to key personnel.

f. Organizational Conflicts of Interest: Where there may be an organizational conflict of interest as determined by the ordering agency, the Contractor's participation in such order may be restricted in accordance with FAR Part 9.5.

g. Documentation/Standards: The Contractor may be requested to provide products or services in accordance with rules, regulations, OMB orders, standards and documentation as specified by the agency's order.

h. Data/Deliverable Requirements: Any required data/deliverables at the ordering level will be as specified or negotiated in the agency's order.

i. Government-Furnished Property: As specified by the agency's order, the Government may provide property, equipment, materials or resources as necessary.

j. Availability of Funds: Many Government agencies' operating funds are appropriated for a specific fiscal year. Funds may not be presently available for any orders placed under the contract or any option year. The Government's obligation on orders placed under this contract is contingent upon the availability of appropriated funds from which payment for ordering purposes can be made. No legal liability on the part of the Government for any payment may arise until funds are available to the ordering Contracting Officer.

15. CONTRACT ADMINISTRATION FOR ORDERING ACTIVITIES: Any ordering activity, with respect to any one or more delivery orders placed by it under this contract, may exercise the same rights of termination as might the GSA Contracting Officer under provisions of FAR 52.212-4, paragraphs (l) Termination for the ordering activity's convenience, and (m) Termination for Cause (See C.1.)

16. GSA Advantage!

GSA Advantage! is an on-line, interactive electronic information and ordering system that provides on-line access to vendors' schedule prices with ordering information. GSA Advantage! will allow the user to perform various searches across all contracts including, but not limited to:

(1) Manufacturer;

(2) Manufacturer's Part Number; and

(3) Product categories.

Agencies can browse GSA Advantage! by accessing the Internet World Wide Web utilizing a browser (ex.: Netscape). The Internet address is http://www.fss.gsa.gov/.

17. PURCHASE OF OPEN MARKET ITEMS

NOTE: Open Market Items are also known as incidental items, noncontract items, non-Schedule items, and items not on a Federal Supply Schedule contract. ODCs (Other Direct Costs) are not part of this contract and should be treated at open market purchases. Ordering Activities procuring open market items must follow FAR 8.401(d).

For administrative convenience, an ordering activity contracting officer may add items not on the Federal Supply Multiple Award Schedule (MAS) -- referred to as open market items -- to a Federal Supply Schedule blanket purchase agreement (BPA) or an individual task or delivery order, **only if-**

(1) All applicable acquisition regulations pertaining to the purchase of the items not on the Federal Supply Schedule have been followed (e.g., publicizing (Part 5), competition requirements (Part 6), acquisition of commercial items (Part 12), contracting methods (Parts 13, 14, and 15), and small business programs (Part 19));

(2) The ordering activity contracting officer has determined the price for the items not on the Federal Supply Schedule is fair and reasonable;

(3) The items are clearly labeled on the order as items not on the Federal Supply Schedule; and

(4) All clauses applicable to items not on the Federal Supply Schedule are included in the order.

18. CONTRACTOR COMMITMENTS, WARRANTIES AND REPRESENTATIONS

a. For the purpose of this contract, commitments, warranties and representations include, in addition to those agreed to for the entire schedule contract:

(1) Time of delivery/installation quotations for individual orders;

(2) Technical representations and/or warranties of products concerning performance, total system performance and/or configuration, physical, design and/or functional characteristics and capabilities of a product/equipment/ service/software package submitted in response to requirements which result in orders under this schedule contract.

(3) Any representations and/or warranties concerning the products made in any literature, description, drawings and/or specifications furnished by the Contractor.

b. The above is not intended to encompass items not currently covered by the GSA Schedule contract.

19. OVERSEAS ACTIVITIES

The terms and conditions of this contract shall apply to all orders for installation, maintenance and repair of equipment in areas listed in the pricelist outside the 48 contiguous states and the District of Columbia, except as indicated below:

Not Applicable

Upon request of the Contractor, the ordering activity may provide the Contractor with logistics support, as available, in accordance with all applicable ordering activity regulations. Such ordering activity support will be provided on a reimbursable basis, and will only be provided to the Contractor's technical personnel whose services are exclusively required for the fulfillment of the terms and conditions of this contract.

20. BLANKET PURCHASE AGREEMENTS (BPAs)

Federal Acquisition Regulation (FAR) 13.303-1(a) defines Blanket Purchase Agreements (BPAs) as "…a simplified method of filling anticipated repetitive needs for supplies or services by establishing 'charge accounts' with qualified sources of supply." The use of Blanket Purchase Agreements under the Federal Supply Schedule Program is authorized in accordance with FAR 13.303-2(c)(3), which reads, in part, as follows:

"BPAs may be established with Federal Supply Schedule Contractors, if not inconsistent with the terms of the applicable schedule contract."

Federal Supply Schedule contracts contain BPA provisions to enable schedule users to maximize their administrative and purchasing savings. This feature permits schedule users to set up "accounts" with Schedule Contractors to fill recurring requirements. These accounts establish a period for the BPA and generally address issues such as the frequency of ordering and invoicing, authorized callers, discounts, delivery locations and times. Agencies may qualify for the best quantity/volume discounts available under the contract, based on the potential volume of business that may be generated through such an agreement, regardless of the size of the individual orders. In addition, agencies may be able to secure a discount higher than that available in the contract based on the aggregate volume of business possible under a BPA. Finally, Contractors may be open to a progressive type of discounting where the discount would increase once the sales accumulated under the BPA reach certain prescribed levels. Use of a BPA may be particularly useful with the new Maximum Order feature. See the Suggested Format, contained in this Schedule Pricelist, for customers to consider when using this purchasing tool.

21. CONTRACTOR TEAM ARRANGEMENTS

Contractors participating in contractor team arrangements must abide by all terms and conditions of their respective contracts. This includes compliance with Clauses 552.238-74, Industrial Funding Fee and Sales Reporting, i.e., each contractor (team member) must report sales and remit the IFF for all products and services provided under its individual contract.

22. INSTALLATION, DEINSTALLATION, REINSTALLATION

The Davis-Bacon Act (40 U.S.C. 276a-276a-7) provides that contracts in excess of $2,000 to which the United States or the District of Columbia is a party for construction, alteration, or repair (including painting and decorating) of public buildings or public works with the United States, shall contain a clause that no laborer or mechanic employed directly upon the site of the work shall received less than the prevailing wage rates as determined by the Secretary of Labor. The requirements of the Davis-Bacon Act do not apply if the construction work is incidental to the furnishing of supplies, equipment, or services. For example, the requirements do not apply to simple installation or alteration of a public building or public work that is incidental to furnishing supplies or equipment under a supply contract. However, if the construction, alteration or repair is segregable and exceeds $2,000, then the requirements of the Davis-Bacon Act applies.
The ordering activity issuing the task order against this contract will be responsible for proper administration and enforcement of the Federal labor standards covered by the Davis-Bacon Act. The proper Davis-Bacon wage determination will be issued by the ordering activity at the time a request for quotations is made for applicable construction classified installation, deinstallation, and reinstallation services under SIN 132-8.

23. SECTION 508 COMPLIANCE.

If applicable, Section 508 compliance information on the supplies and services in this contract are available in Electronic and Information Technology (EIT) at the following:

Not Applicable

The EIT standard can be found at: www.Section508.gov/.

24. PRIME CONTRACTOR ORDERING FROM FEDERAL SUPPLY SCHEDULES.

Prime Contractors (on cost reimbursement contracts) placing orders under Federal Supply Schedules, on behalf of an ordering activity, shall follow the terms of the applicable schedule and authorization and include with each order –

a. A copy of the authorization from the ordering activity with whom the contractor has the prime contract (unless a copy was previously furnished to the Federal Supply Schedule contractor); and

b. The following statement:

This order is placed under written authorization from _N/A_ dated _N/A_. In the event of any inconsistency between the terms and conditions of this order and those of your Federal Supply Schedule contract, the latter will govern.

25. INSURANCE—WORK ON A GOVERNMENT INSTALLATION (JAN 1997)(FAR 52.228-5)

a. The Contractor shall, at its own expense, provide and maintain during the entire performance of this contract, at least the kinds and minimum amounts of insurance required in the Schedule or elsewhere in the contract.

b. Before commencing work under this contract, the Contractor shall notify the Contracting Officer in writing that the required insurance has been obtained. The policies evidencing required insurance shall contain an endorsement to the effect that any cancellation or any material change adversely affecting the Government's interest shall not be effective—

(1) For such period as the laws of the State in which this contract is to be performed prescribe; or

(2) Until 30 days after the insurer or the Contractor gives written notice to the Contracting Officer, whichever period is longer.

c. The Contractor shall insert the substance of this clause, including this paragraph (c), in subcontracts under this contract that require work on a Government installation and shall require subcontractors to provide and maintain the insurance required in the Schedule or elsewhere in the contract. The Contractor shall maintain a copy of all subcontractors' proofs of required insurance, and shall make copies available to the Contracting Officer upon request.

TERMS AND CONDITIONS APPLICABLE TO LEASING OF GENERAL PURPOSE COMMERCIAL INFORMATION TECHNOLOGY PRODUCTS (SPECIAL ITEM NUMBER 132-3)

LEASE TYPES

The ordering activity will consider proposals for the following lease types:

a. Lease to Ownership,

b. Lease with Option to Own, and

c. Step Lease.

Orders for leased products must specify the leasing type.

OPTION 1:

1. STATEMENT

a. It is understood by all parties to this contract that orders issued under this SIN shall constitute a lease arrangement. Unless the ordering activity intends to obligate other than annual appropriations to fund the lease, the base period of the lease is from the date of the product acceptance through September 30 of the fiscal year in which the order is placed.

b. Agencies are advised to follow the guidance provided in Federal Acquisition Regulation (FAR) Subpart 7.4 Product Lease or Purchase and OMB Circular A-11. Agencies are responsible for the obligation of funding consistent with all applicable legal principles when entering into any lease arrangement.

2. FUNDING AND PERIODS OF LEASING ARRANGEMENTS

(a) Annual Funding. When annually appropriated funds are cited on an order for leasing, the following applies:

(1) The base period of an order for any lease executed by the ordering activity shall be for the duration of the fiscal year. All ordering activity renewal options under the lease shall be specified in the delivery order. All orders for leasing shall remain in effect through September 30 of the fiscal year or the planned expiration date of the lease, whichever is earlier, unless the ordering activity exercises its rights hereunder to acquire title to the product prior to the planned expiration date or unless the ordering activity exercise its right to terminate under FAR 52.212-4. Orders under the lease shall not be deemed to obligate succeeding fiscal year's funds or to otherwise commit the ordering activity to a renewal.

(2) All orders for leasing shall automatically terminate on September 30, unless the ordering activity notifies the Contractor in writing thirty (30) calendar days prior to the expiration of such orders of the ordering activity's intent to renew. Such notice to renew shall not bind the ordering activity. The ordering activity has the

option to renew each year at the original rate in effect at the time the order is placed. This rate applies for the duration of the order. If the ordering activity exercises its option to renew, the renewal order, shall be issued within 15 days after funds become available for obligation by the ordering activity, or as specified in the initial order. No termination fees shall apply if the ordering activity does not exercise an option.

(b) Crossing Fiscal Years Within Contract Period. Where an ordering activity has specific authority to cross fiscal years with annual appropriations, the ordering activity may place an order under this option to lease product for a period up to the expiration of its period of appropriation availability, or twelve months, whichever occurs later, notwithstanding the intervening fiscal years.

3. DISCONTINUANCE AND TERMINATION

Notwithstanding any other provision relating to this SIN, the ordering activity may terminate products leased under this agreement, at any time during a fiscal year in accordance with the termination provisions contained in FAR 52.212-4. (l) Termination for the ordering activity’s convenience, or (m) Termination for cause. Additionally, no termination for cost or fees shall be charged for non-renewal of an option.

****

OPTION 2

To the extent an Offeror wishes to propose alternative lease terms and conditions that provide for lower discounts/prices based on the ordering activity’s stated intent to fulfill the projected term of a lease including option years, while at the same time including separate charges for early end of the lease, the following terms apply. These terms address the timing and extent of the ordering activity’s financial obligation including any potential charges for early end of the lease.

1. LEASING PRICE LIST NOTICE:

Contractors must include the following notice in their contract price list for SIN 132-3:

“The ordering activity is responsible for the obligation of funds consistent with applicable law. Agencies are advised to review the lease terms and conditions contained in this price list prior to ordering and obligating funding for a lease.”

2. STATEMENT OF ORDERING ACTIVITY INTENT:

(a) The ordering activity and the Contractor understand that a delivery order issued pursuant to this SIN is a lease arrangement and contemplates the use of the product for the term of the lease specified in such delivery order (the “Lease Term”). In that regard, the ordering Activity, as lessee, understands that the lease provisions contained herein and the rate established for the delivery order are premised on the ordering Activity's intent to fulfill that agreement, including acquiring products for the period of time specified in the order. Each lease hereunder shall be initiated by a delivery order which shall, either through a statement of work or other attachment, specify the product being leased, and the required terms of the transaction.

(b) Each ordering activity placing a delivery order under the terms of this option intends to exercise each renewal option and to extend the lease until completion of the Lease Term so long as the need of the ordering activity for the product or functionally similar product continues to exist and funds are appropriated. Contractor may request information from the ordering activity concerning the essential use of the products.

3. LEASE TERM:

(a) The date on which the ordering activity accepts the products is the Commencement Date of the lease. For acceptance to occur, the products must operate in accordance with the product’s published specifications and statement of work. Acceptance shall be in accordance with the terms of the contract or as otherwise negotiated by the ordering activity and the Contractor.

(b) Any lease is executed by the ordering activity on the basis that the known requirement for such product exceeds the initial base period of the delivery order, which is typically 12 months, or for the remainder of the fiscal year. Pursuant to FAR 32.703-3(b), delivery orders with options to renew that are funded by annual (fiscal year) appropriations may provide for initial base periods and option periods that cross fiscal years as long as the initial base period or each option period does not exceed a 12 month period. Defense agencies must also consider DOD FAR supplement (DFAR) 232.703-3(b) in determining whether to use cross fiscal year funding. This cross fiscal year authority does not apply to multi-year leases.

(c) The total Lease Term will be specified in each delivery order, including any relevant renewal options of the ordering activity. All delivery orders, whether for the initial base period or renewal period, shall remain in effect through September 30 of the fiscal year (unless extended by statute), through any earlier expiration date specified in the delivery order, or until the ordering activity exercises its rights hereunder to acquire title to the product prior to such expiration date. The ordering activity, at its discretion, may exercise each option to extend the term of the lease through the lease term. Renewal delivery orders shall not be issued for less than all of the product and/or software set forth in the original delivery order**.** Delivery orders under this SIN shall not be deemed to obligate succeeding fiscal year funds. The ordering activity shall provide the Contractor with written notice of exercise of each renewal option as soon as practicable. Notice requirements may be negotiated on an order-by-order basis.

(d) Where an ordering activity's specific appropriation or procurement authority provides for contracting beyond the fiscal year period, the ordering activity may place a delivery order for a period up to the expiration of the Lease Term, or to the expiration of the period of availability of the multi-year appropriation, or whatever is appropriate under the applicable circumstance.

4. LEASE TERMINATION:

(a) The ordering activity must elect the Lease Term of the relevant delivery order. The Contractor (and assignee, if any) will rely on the ordering activity's representation of its intent to fulfill the full Lease Term to determine the monthly lease payments calculated herein.

(i) The ordering activity may terminate or not renew leases under this option at no cost, pursuant to a Termination for Non-Appropriation as defined herein (see paragraph (c) below). In any other event, the ordering activity's contracting officer may either terminate the relevant delivery order for cause or Termination for Convenience in accordance with FAR 52.212-4 paragraphs (l) and (m).

(ii) The Termination for Convenience at the end of a fiscal year allows for separate charges for the early end of the lease (see paragraph (d) below). In the event of termination for the convenience of the ordering activity, the ordering activity may be liable only up to the amount beyond the order's Termination Ceiling. Any termination charges calculated under the Termination for Convenience clause must be determined or identified in the delivery order or in the lease agreement.

(b) Termination for Convenience of the Ordering Activity**:** Leases entered into under this option may not be terminated except by the ordering activity's contracting office responsible for the delivery order in accordance with FAR 52.212-4, Contract Terms and Conditions-Commercial Items, paragraph (l), *Termination for Convenience of the ordering activity*. The costs charged to the ordering activity as the result of any Termination for Convenience of the ordering activity must be reasonable and may not exceed the sum of the fiscal year's payment obligations less payments made to date of termination plus the Termination Ceiling

(c) Termination for Non-Appropriation: The ordering activity reasonably believes that the bona fide need will exist for the entire Lease Term and corresponding funds in an amount sufficient to make all payment for the lease Term will be available to the ordering activity. Therefore, it is unlikely that leases entered into under this option will terminate prior to the full Lease Term. Nevertheless, the ordering activity's contracting officer may terminate or not renew leases at the end of any initial base period or option period under this paragraph if (a) it no longer has a bona fide need for the product or functionally similar product; or (b) there is a continuing need, but adequate funds have not been made available to the ordering activity in an amount sufficient to continue to make the lease payments. If this occurs, the ordering activity will promptly notify the Contractor, and the product lease will be terminated at the end of the last fiscal year for which funds were appropriated. Substantiation to support a termination for non-appropriation shall be provided to the Contractor upon request.

(d) Termination Charges: At the initiation of the lease, termination ceilings will be established for each year of the lease term. The termination ceiling is a limit on the amount that a Contractor may be paid by the ordering activity on the Termination for Convenience of a lease. No claim will be accepted for future costs: supplies, maintenance, usage charges or interest expense beyond the date of termination. In accordance with the bona fide needs rule, all termination charges must reasonably represent the value the ordering activity received for the work performed based upon the shorter lease term. No Termination for Convenience costs will be associated with the expiration of the lease term.

(e) At the order level, the ordering activity may, consistent with legal principles, negotiate lower monthly payments or rates based upon appropriate changes to the termination conditions in this section.

****

LEASE PROVISIONS COMMON TO
ALL TYPES OF LEASE AGREEMENTS

1. ORDERING PROCEDURES:

(a) When an ordering activity expresses an interest in leasing a product(s), the ordering activity will provide the following information to the prospective Contractor:

(i) Which product(s) is (are) required.
(ii) The required delivery date.
(iii) The proposed lease plan and term of the lease.
(iv) Where the product will be located.
(v) Description of the intended use of the product.
(vi) Source and type of appropriations to be used.

(b) The Contractor will respond with:

(i) Whether the Contractor can provide the required product.
(ii) The estimated residual value of the product (Lease with Option to Own and Step Lease only).
(iii) The monthly payment based on the rate.
(iv) The estimated cost, if any, of applicable State or local taxes. State and local personal property taxes are to be estimated as separate line items in accordance with FAR 52.229-1, which may be identified and added to the monthly lease payment.
(v) A confirmation of the availability of the product on the required delivery date.
(vi) Extent of warranty coverage, if any, of the leased products.
(vii) The length of time the quote is valid.

(c) The ordering activity may issue a delivery order to the Contractor based on the information set forth in the Contractor's quote. In the event that the ordering activity does not issue a delivery order within the validity period stated in the Contractor's quote letter, the quote shall expire.

2. ASSIGNMENT OF CLAIMS:

GSAR 552.232-23, Assignment of Claims, is incorporated herein by reference as part of these lease provisions. The ordering activity's contracting officer will acknowledge the assignment of claim for a lease in accordance with FAR 32.804-5. The extent of the assignee's protection is in accordance with FAR 32.804. Any setoff provision must be in accordance with FAR 32.803.

3. PEACEFUL POSSESSION AND UNRESTRICTED USE:

In recognition of the types of products available for lease and the potential adverse impact to the ordering activity's mission, the ordering activity's quiet and peaceful possession and unrestricted use of the product shall not be disturbed in the event the product is sold by the Contractor, or in the event of bankruptcy of the Contractor, corporate dissolution of the Contractor, or other event. The product shall remain in the possession of the ordering activity until the expiration of the lease. Any assignment, sale, bankruptcy, or other transfer of the leased product by the Contractor will not relieve the Contractor of its obligations to the ordering activity, and will not change the ordering activity's duties or increase the burdens or risks imposed on the ordering activity.

4. COMMENCEMENT OF LEASE:

The date on which the ordering activity accepts the products is the Commencement Date of the lease. Acceptance is as defined elsewhere in the contract, or as further specified in the order.

5. INSTALLATION AND MAINTENANCE:

a. Installation and Maintenance, when applicable, normally are not included in the charge for leasing. The Contractor may require the ordering activity to obtain installation and maintenance services from a qualified source. The ordering activity may obtain installation and/or maintenance on the open market, from the Contractor's schedule contract, or from other sources. The ordering activity may also perform installation and/or maintenance in house, if qualified resources exist. In any event, it is the responsibility of the ordering activity to ensure that maintenance is in effect for the Lease term for all products leased.

b. When installation and/or maintenance are ordered under this schedule to be performed by the Contractor, the payments, terms and conditions as stated in this contract apply. The rates and terms and conditions in effect at the time the order is issued shall apply during any subsequent renewal period of the lease. The maintenance rates and terms and conditions may be added to the lease payments with mutual agreement of the parties.

6. MONTHLY PAYMENTS:

a. Prior to the placement of an order under this Special Item Number, the ordering activity and the Contractor must agree on a "base value" for the products to be leased. For Lease to Ownership (Capital Lease) the base value will be the contract purchase price (less any discounts). For Lease with Option to Own (Operating Lease), the base value will be the contract purchase price (less any discounts), less a mutually agreed upon residual value (pre-stated purchase option price at the conclusion of the lease) for the products. The residual value will be used in the calculation of the original lease payment, lease extension payments, and the purchase option price.

b. To determine the initial lease term payment, the Contractor agrees to apply the negotiated lease factor to the agreed upon base value:

____

For Example:Lease factor one (1) percent over the rate for the three year (or other term) Treasury Bill (T-bill) at the most current U. S. Treasury auction.

The lease payment may be calculated by using a programmed business calculator or by using "rate" functions provided in commercial computer spreadsheets (e.g., Lotus 1-2-3, Excel).

c. For any lease extension, the extension lease payment will be based on the original residual value, in lieu of the purchase price. The ordering activity and the Contractor shall agree on a new residual value based on the estimated fair market price at the end of the extension. The formula to determine the lease payment will be that in 6.b. above.

d. The purchase option price will be the fair market value of the product or payment will be based upon the unamortized principle, as shown on the payment schedule as of the last payment prior to date of transfer of ownership, whichever is less.

NOTE: At the order level, ordering activity may elect to obtain a lower rate for the lease by setting the purchase option price as either, the fair market value of the product or unamoritized principle. The methodology for determining lump sum payments may be identified in the pricelist.

e. The point in time when monthly rates are established is subject to negotiation and evaluation at the order level.

In the event the ordering activity desires, at any time, to acquire title to product leased hereunder, the ordering activity may make a one-time lump sum payment.

7. LEASE END/DISCONTINUANCE OPTIONS:

a. Upon the expiration of the Lease Term, Termination for Convenience, or Termination for NonAppropriation, the ordering activity will return the Product to the Contractor unless the ordering activity by 30 days written notice elects either:

(i) to purchase the product for the residual value of the product, or

(ii) to extend the term of the Lease, as mutually agreed. To compute the lease payment, the residual value from the preceding lease shall be the initial value of the leased product. A new residual value shall be negotiated for the extended lease and new lease payments shall be computed.

b. Relocation - The ordering activity may relocate products to another location within the ordering activity with prior written notice. No other transfer, including sublease, is permitted. Ordering activity shall not assign, transfer or otherwise dispose of any products, or any interest therein, or crate or suffer any levy, lien or encumbrance then except those created for the benefit of Contractor or it's assigns.

c. Returns:

(i) Within fourteen (14) days after the date of expiration, non-renewal or termination of a lease, the ordering activity shall, at its own risk and expense, have the products packed for shipment in accordance with manufacturer's specifications and return the products to Contractor at the location specified by Contractor in the continental US, in the same condition as when delivered, ordinary wear and tear excepted. Any expenses necessary to return the products to good working order shall be at ordering activity's expense.

(ii) The Contractor shall conduct a timely inspection of the returned products and within 45 days of the return, assert a claim if the condition of the product exceeds normal wear and tear.

(iii) Product will be returned in accordance with the terms of the contract and in accordance with Contractor instruction.

(iv) With respect to software, the ordering activity shall state in writing to the Contractor that it has:

(1) deleted or disabled all files and copies of the software from the equipment on which it was installed;

(2) returned all software documentation, training manuals, and physical media on which the software was delivered; and

(3) has no ability to use the returned software.

8. UPGRADES AND ADDITIONS:

a. The ordering activity may affix or install any accessory, addition, upgrade, product or device on the product ("additions") provided that such additions:

(1) can be removed without causing material damage to the product;

(2) do not reduce the value of the product; and

(3) are obtained from or approved by the Contractor, and are not subject to the interest of any third party other than the Contractor.

b. Any other additions may not be installed without the Contractor's prior written consent. At the end of the lease term, the ordering activity shall remove any additions which:

(1) were not leased from the Contractor, and

(2) are readily removable without causing material damage or impairment of the intended function, use, or value of the product, and restore the product to its original configuration.

c. Any additions that are not so removable will become the Contractor's property (lien free).

d. Leases of additions and upgrades must be co-terminus with that of the product.

9. RISK OF LOSS OR DAMAGE:

The ordering activity is relieved from all risk of loss or damage to the product during periods of transportation, installation, and during the entire time the product is in possession of the ordering activity, except when loss or damage is due to the fault or negligence of the ordering activity. The ordering activity shall assume risk of loss or damage to the product during relocation, (i.e., moving the product from one ordering activity location to another ordering activity location), unless the Contractor shall undertake such relocation.

10. TITLE:

During the lease term, product shall always remain the property of the Contractor. The ordering activity shall have no property right or interest in the product except as provided in this leasing agreement and shall hold the product subject and subordinate to the rights of the Contractor. Software and software licenses shall be deemed personal property. The ordering activity shall have no right or interest in the software and related documentation except as provided in the license and the lease. Upon the Commencement Date of the Lease Term, the ordering activity shall have an encumbered license to use the software for the Lease Term. The ordering activity's encumbered license rights in the software will be subject to the same rights as provided to a purchaser of a license under the terms of this contract except that the ordering activity will not have an unencumbered, paid-up license until it has made all lease payments for the full Lease Term in the case of an Lease To Ownership or has otherwise paid the applicable purchase option price.

11. TAXES:

The lease payments, purchase option prices, and interest rates identified herein exclude all state and local taxes levied on or measured by the contract or sales price of the product furnished hereunder. The ordering activity will be invoiced for any such taxes as Contractor receives such tax notices or assessments from the applicable local taxing authority. Pursuant to the provisions of FAR 52.229-1 (Deviation – May 2003), State and Local Taxes, the ordering activity agrees to pay tax or provide evidence necessary to support an exemption from the tax.

12. OPTION TO PURCHASE EQUIPMENT (FEB 1995) (FAR 52.207-5)

(a) The Government may purchase the equipment provided on a lease or rental basis under this contract. The Contracting Officer may exercise this option only by providing a unilateral modification to the Contractor. The effective date of the purchase will be specified in the unilateral modification and may be any time during the period of the contract, including any extensions thereto.

(b) Except for final payment and transfer of title to the Government, the lease or rental portion of the contract becomes complete and lease or rental charges shall be discontinued on the day immediately preceding the effective date of purchase specified in the unilateral modification required in paragraph (a) of this clause.

(c) The purchase conversion cost of the equipment shall be computed as of the effective date specified in the unilateral modification required in paragraph (a) of this clause, on the basis of the purchase price set forth in the contract, minus the total purchase option credits accumulated during the period of lease or rental, calculated by the formula contained elsewhere in this contract.

(d) The accumulated purchase option credits available to determine the purchase conversion cost will also include any credits accrued during a period of lease or rental of the equipment under any previous Government contract if the equipment has been on continuous lease or rental. The movement of equipment from one site to another site shall be “continuous rental.”

TERMS AND CONDITIONS APPLICABLE TO TERM SOFTWARE LICENSES (SPECIAL ITEM NUMBER 132-32) AND MAINTENANCE (SPECIAL ITEM NUMBER 132-34) OF GENERAL PURPOSE COMMERCIAL INFORMATION TECHNOLOGY SOFTWARE

1. INSPECTION/ACCEPTANCE

The Contractor shall only tender for acceptance those items that conform to the requirements of this contract. The ordering activity reserves the right to inspect or test any software that has been tendered for acceptance. The ordering activity may require repair or replacement of nonconforming software at no increase in contract price. The ordering activity must exercise its postacceptance rights (1) within a reasonable time after the defect was discovered or should have been discovered; and (2) before any substantial change occurs in the condition of the software, unless the change is due to the defect in the software.

2. GUARANTEE/WARRANTY

a. Unless specified otherwise in this contract, the Contractor's standard commercial guarantee/warranty as stated in the contract's commercial pricelist will apply to this contract.

The contractor will provide a 90-day warranty with purchase of product. A one-year warranty is provided with the purchase of annual maintenance.

b. The Contractor warrants and implies that the items delivered hereunder are merchantable and fit for use for the particular purpose described in this contract.

c. Limitation of Liability. Except as otherwise provided by an express or implied warranty, the Contractor will not be liable to the ordering activity for consequential damages resulting from any defect or deficiencies in accepted items.

3. TECHNICAL SERVICES

The Contractor, without additional charge to the ordering activity, shall provide a hot line technical support number **1-888-428-4333** or by e-mail to **support@ securityassociatescorp.com** for the purpose of providing user assistance and guidance in the implementation of the software. The technical support number is available from **9:00 AM to 9:00 PM Eastern Time**.

4. SOFTWARE MAINTENANCE

a. Software maintenance service shall include the following:

(1) Technical assistance with the all software issues, including patches and updates during the annual maintenance period.

(2) E-mail assistance is also provided.

b. Invoices for maintenance service shall be submitted by the Contractor on a quarterly or monthly basis, after the completion of such period. Maintenance charges must be paid in arrears (31 U.S.C. 3324). PROMPT PAYMENT DISCOUNT, IF APPLICABLE, SHALL BE SHOWN ON THE INVOICE.

5. PERIODS OF TERM LICENSES (132-32) AND MAINTENANCE (132-34)

a. The Contractor shall honor orders for periods for the duration of the contract period or a lesser period of time.

b. Term licenses and/or maintenance may be discontinued by the ordering activity on thirty (30) calendar days written notice to the Contractor.

c. Annual Funding. When annually appropriated funds are cited on an order for term licenses and/or maintenance, the period of the term licenses and/or maintenance shall automatically expire on September 30 of the contract period, or at the end of the contract period, whichever occurs first. Renewal of the term licenses and/or maintenance orders citing the new appropriation shall be required, if the term licenses and/or maintenance is to be continued during any remainder of the contract period.

d. Cross-Year Funding Within Contract Period. Where an ordering activity's specific appropriation authority provides for funds in excess of a 12 month (fiscal year) period, the ordering activity may place an order under this schedule contract for a period up to the expiration of the contract period, notwithstanding the intervening fiscal years.

e. Ordering activities should notify the Contractor in writing thirty (30) calendar days prior to the expiration of an order, if the term licenses and/or maintenance is to be terminated at that time. Orders for the continuation of term licenses and/or maintenance will be required if the term licenses and/or maintenance is to be continued during the subsequent period.

6. CONVERSION FROM TERM LICENSE TO PERPETUAL LICENSE

Term software provided under the scope of this contract cannot be converted to perpetual license software.

7. TERM LICENSE CESSATION

Term software provided under the scope of this contract cannot be converted to perpetual license software.

8. UTILIZATION LIMITATIONS - (132-32, 132-33, AND 132-34)

a. Software acquisition is limited to commercial computer software defined in FAR Part 2.101.

b. When acquired by the ordering activity, commercial computer software and related documentation so legend shall be subject to the following:

(1) Title to and ownership of the software and documentation shall remain with the Contractor, unless otherwise specified.

(2) Software licenses are by site and by ordering activity. An ordering activity is defined as a cabinet level or independent ordering activity. The software may be used by any subdivision of the ordering activity (service, bureau, division, command, etc.) that has access to the site the software is placed at, even if the subdivision did not participate in the acquisition of the software. Further, the software may be used on a sharing basis where multiple agencies have joint

projects that can be satisfied by the use of the software placed at one ordering activity's site. This would allow other agencies access to one ordering activity's database. For ordering activity public domain databases, user agencies and third parties may use the computer program to enter, retrieve, analyze and present data. The user ordering activity will take appropriate action by instruction, agreement, or otherwise, to protect the Contractor's proprietary property with any third parties that are permitted access to the computer programs and documentation in connection with the user ordering activity's permitted use of the computer programs and documentation. For purposes of this section, all such permitted third parties shall be deemed agents of the user ordering activity.

(3) Except as is provided in paragraph 8.b(2) above, the ordering activity shall not provide or otherwise make available the software or documentation, or any portion thereof, in any form, to any third party without the prior written approval of the Contractor. Third parties do not include prime Contractors, subcontractors and agents of the ordering activity who have the ordering activity's permission to use the licensed software and documentation at the facility, and who have agreed to use the licensed software and documentation only in accordance with these restrictions. This provision does not limit the right of the ordering activity to use software, documentation, or information therein, which the ordering activity may already have or obtains without restrictions.

(4) The ordering activity shall have the right to use the computer software and documentation with the computer for which it is acquired at any other facility to which that computer may be transferred, or in cases of disaster recovery, the ordering activity has the right to transfer the software to another site if the ordering activity site for which it is acquired is deemed to be unsafe for ordering activity personnel; to use the computer software and documentation with a backup computer when the primary computer is inoperative; to copy computer programs for safekeeping (archives) or backup purposes; to transfer a copy of the software to another site for purposes of benchmarking new hardware and/or software; and to modify the software and documentation or combine it with other software, provided that the unmodified portions shall remain subject to these restrictions.

(5) "Commercial Computer Software" may be marked with the Contractor’s standard commercial restricted rights legend, but the schedule contract and schedule pricelist, including this clause, "Utilization Limitations" are the only governing terms and conditions, and shall take precedence and supersede any different or additional terms and conditions included in the standard commercial legend.

9. SOFTWARE CONVERSIONS - (132-32 AND 132-33)

Software conversions are not applicable under the scope of this contract.

10. DESCRIPTIONS AND EQUIPMENT COMPATIBILITY

The Contractor shall include, in the schedule pricelist, a complete description of each software product and a list of equipment on which the software can be used. Also, included shall be a brief, introductory explanation of the modules and documentation which are offered.

11. RIGHT-TO-COPY PRICING

Right-To-Copy is not applicable under the scope of this contract.

TERMS AND CONDITIONS APPLICABLE TO PURCHASE OF TRAINING COURSES FOR GENERAL PURPOSE COMMERCIAL INFORMATION TECHNOLOGY EQUIPMENT AND SOFTWARE (SPECIAL ITEM NUMBER 132-50)

1. SCOPE

a. The Contractor shall provide training courses normally available to commercial customers, which will permit ordering activity users to make full, efficient use of general purpose commercial IT products. Training is restricted to training courses for those products within the scope of this solicitation.

b. The Contractor shall provide training at the Contractor's facility and/or at the ordering activity's location, as agreed to by the Contractor and the ordering activity.

2. ORDER

Written orders, EDI orders (GSA Advantage! and FACNET), credit card orders, and orders placed under blanket purchase agreements (BPAs) shall be the basis for the purchase of training courses in accordance with the terms of this contract. Orders shall include the student's name, course title, course date and time, and contracted dollar amount of the course.

3. TIME OF DELIVERY

The Contractor shall conduct training on the date (time, day, month, and year) agreed to by the Contractor and the ordering activity.

4. CANCELLATION AND RESCHEDULING

a. The ordering activity will notify the Contractor at least seventy-two (72) hours before the scheduled training date, if a student will be unable to attend. The Contractor will then permit the ordering activity to either cancel the order or reschedule the training at no additional charge. In the event the training class is rescheduled, the ordering activity will modify its original training order to specify the time and date of the rescheduled training class.

(1) Training is paid prior to the commencement of classes.

(2) Training dates can be rescheduled up to 3 times within 30 days from initial agreed upon date and time at no extra charge.

(3) After 30 days a fee may be assessed in addition to any cost associated with travel rescheduling.

b. In the event the ordering activity fails to cancel or reschedule a training course within the time frame specified in paragraph a, above, the ordering activity will be liable for the contracted dollar amount of the training course. The Contractor agrees to permit the ordering activity to reschedule a student who fails to attend a training class within ninety (90) days from the original course date, at no additional charge.

c. The ordering activity reserves the right to substitute one student for another up to the first day of class.

d. In the event the Contractor is unable to conduct training on the date agreed to by the Contractor and the ordering activity, the Contractor must notify the ordering activity at least seventy-two (72) hours before the scheduled training date.

5. FOLLOW-UP SUPPORT

Contractor provides a trouble ticketing system that tracks all trouble calls or e-mails based on an assigned priority. All trouble calls are tracked to resolution or work around depending on the priority assigned to the customer call.

6. PRICE FOR TRAINING

The price that the ordering activity will be charged will be the ordering activity training price in effect at the time of order placement, or the ordering activity price in effect at the time the training course is conducted, whichever is less.

7. INVOICES AND PAYMENT

Invoices for training shall be submitted by the Contractor after ordering activity completion of the training course. Charges for training must be paid in arrears (31 U.S.C. 3324). PROMPT PAYMENT DISCOUNT, IF APPLICABLE, SHALL BE SHOWN ON THE INVOICE.

8. FORMAT AND CONTENT OF TRAINING

a. The Contractor shall provide written materials (i.e., manuals, handbooks, texts, etc.) normally provided with course offerings. Such documentation will become the property of the student upon completion of the training class.

b. For hands-on training courses, there must be a one-to-one assignment of IT equipment to students.

c. The Contractor shall provide each student with a Certificate of Training at the completion of each training course.

d. The Contractor shall provide the following information for each training course offered:

(1) The course title and a brief description of the course content, to include the course format (e.g., lecture, discussion, hands-on training);

Enterprise Contract Management Introductory Training –This is a hands-on training for the use of the ECM software.

(2) The length of the course;

This is a two-day training course.

(3) Mandatory and desirable prerequisites for student enrollment;

No prerequisites.

(4) The minimum and maximum number of students per class;

Maximum of fifteen (15) students per class. There is no minimum number of students. There is no limit to online training classes.

(5) The locations where the course is offered;

Course is offered at customer site or a customer paid training center that has a sufficient number of Internet connected PCs for all students and instructors.

(6) Class schedules; and

Normal training hours are 8:00 AM to 5:00 PM with breaks and 1 hour for lunch.

(7) Price (per student, per class (if applicable)).

Per class price is dependent upon type of software purchased.

e. For those courses conducted at the ordering activity’s location, instructor travel charges (if applicable), including mileage and daily living expenses, must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Contractors cannot use GSA city pair contracts.

9. “NO CHARGE” TRAINING

The Contractor shall describe any training provided with equipment and/or software provided under this contract, free of charge, in the space provided below.

“No charge” training is applicable only in cases of the purchase of an Enterprise Site License.

TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 132-51)

1. SCOPE

   a. The prices, terms and conditions stated under Special Item Number 132-51 Information Technology Professional Services and Special Item Number 132-52 Electronic Commerce Services apply exclusively to IT/EC Services within the scope of this Information Technology Schedule.

   b. The Contractor shall provide services at the Contractor’s facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity.

2. PERFORMANCE INCENTIVES

   a. Performance incentives may be agreed upon between the Contractor and the ordering activity on individual fixed price orders or Blanket Purchase Agreements under this contract in accordance with this clause.

   b. The ordering activity must establish a maximum performance incentive price for these services and/or total solutions on individual orders or Blanket Purchase Agreements.

   c. Incentives should be designed to relate results achieved by the contractor to specified targets. To the maximum extent practicable, ordering activities shall consider establishing incentives where performance is critical to the ordering activity’s mission and incentives are likely to motivate the contractor. Incentives shall be based on objectively measurable tasks.

3. ORDERING PROCEDURES FOR SERVICES (REQUIRING A STATEMENT OF WORK) (G-FCI-920) (MAR 2003)

   FAR 8.402 contemplates that GSA may occasionally find it necessary to establish special ordering procedures for individual Federal Supply Schedules or for some Special Item Numbers (SINs) within a Schedule. GSA has established special ordering procedures for services that require a Statement of Work. These special ordering procedures take precedence over the procedures in FAR 8.404 (b)(2) through (b)(3).

   When ordering services over $100,000, Department of Defense (DOD) ordering offices and non-DOD agencies placing orders on behalf of the DOD must follow the policies and procedures in the Defense Federal Acquisition Regulation Supplement (DFARS) 208.404-70 – Additional ordering procedures for services. When DFARS 208.404-70 is applicable and there is a conflict between the ordering procedures contained in this clause and the additional ordering procedures for services in DFARS 208.404-70, the DFARS procedures take precedence.

   GSA has determined that the prices for services contained in the contractor’s price list applicable to this Schedule are fair and reasonable. However, the ordering activity using this contract is responsible for considering the level of effort and mix of labor proposed to perform a specific task being ordered and for making a determination that the total firm-fixed price or ceiling price is fair and reasonable.

a. When ordering services, ordering activities shall—

(1) Prepare a Request (Request for Quote or other communication tool):

(i) A statement of work (a performance-based statement of work is preferred) that outlines, at a minimum, the work to be performed, location of work, period of performance, deliverable schedule, applicable standards, acceptance criteria, and any special requirements (i.e., security clearances, travel, special knowledge, etc.) should be prepared.

(ii) The request should include the statement of work and request the contractors to submit either a firm-fixed price or a ceiling price to provide the services outlined in the statement of work. A firm-fixed price order shall be requested, unless the ordering activity makes a determination that it is not possible at the time of placing the order to estimate accurately the extent or duration of the work or to anticipate cost with any reasonable degree of confidence. When such a determination is made, a labor hour or time-and-materials proposal may be requested. The firm-fixed price shall be based on the rates in the schedule contract and shall consider the mix of labor categories and level of effort required to perform the services described in the statement of work. The firm-fixed price of the order should also include any travel costs or other incidental costs related to performance of the services ordered, unless the order provides for reimbursement of travel costs at the rates provided in the Federal Travel or Joint Travel Regulations. A ceiling price must be established for labor-hour and time-and-materials orders.

(iii) The request may ask the contractors, if necessary or appropriate, to submit a project plan for performing the task, and information on the contractor's experience and/or past performance performing similar tasks.

(iv) The request shall notify the contractors what basis will be used for selecting the contractor to receive the order. The notice shall include the basis for determining whether the contractors are technically qualified and provide an explanation regarding the intended use of any experience and/or past performance information in determining technical qualification of responses. If consideration will be limited to schedule contractors who are small business concerns as permitted by paragraph (2) below, the request shall notify the contractors that will be the case.

(2) Transmit the Request to Contractors:

Based upon an initial evaluation of catalogs and price lists, the ordering activity should identify the contractors that appear to offer the best value (considering the scope of services offered, pricing and other factors such as contractors' locations, as appropriate) and transmit the request as follows:

NOTE: When buying IT professional services under SIN 132—51 ONLY, the ordering office, at its discretion, may limit consideration to those schedule contractors that are small business concerns. This limitation is not applicable when buying supplies and/or services under other SINs as well as SIN 132-51. The limitation may only be used when at least three (3) small businesses that appear to offer services that will meet the agency's needs are available, if the order is estimated to exceed the micro-purchase threshold.

(i) The request should be provided to at least three (3) contractors if the proposed order is estimated to exceed the micro-purchase threshold, but not exceed the maximum order threshold.

(ii) For proposed orders exceeding the maximum order threshold, the request should be provided to additional contractors that offer services that will meet the ordering activity's needs.

(iii) In addition, the request shall be provided to any contractor who specifically requests a copy of the request for the proposed order.

(iv) Ordering activities should strive to minimize the contractors' costs associated with responding to requests for quotes for specific orders. Requests should be tailored to the minimum level necessary for adequate evaluation and selection for order placement. Oral presentations should be considered, when possible.

(3) Evaluate Responses and Select the Contractor to Receive the Order:

After responses have been evaluated against the factors identified in the request, the order should be placed with the schedule contractor that represents the best value. (See FAR 8.404)

b. The establishment of Federal Supply Schedule Blanket Purchase Agreements (BPAs) for recurring services is permitted when the procedures outlined herein are followed. All BPAs for services must define the services that may be ordered under the BPA, along with delivery or performance time frames, billing procedures, etc. The potential volume of orders under BPAs, regardless of the size of individual orders, may offer the ordering activity the opportunity to secure volume discounts. When establishing BPAs, ordering activities shall—

(1) Inform contractors in the request (based on the ordering activity's requirement) if a single BPA or multiple BPAs will be established, and indicate the basis that will be used for selecting the contractors to be awarded the BPAs.

(i) SINGLE BPA: Generally, a single BPA should be established when the ordering activity can define the tasks to be ordered under the BPA and establish a firm-fixed price or ceiling price for individual tasks or services to be ordered. When this occurs, authorized users may place the order directly under the established BPA when the need for service arises. The schedule contractor that represents the best value should be awarded the BPA. (See FAR 8.404)

(ii) MULTIPLE BPAs: When the ordering activity determines multiple BPAs are needed to meet its requirements, the ordering activity should determine which contractors can meet any technical qualifications before establishing the BPAs. When establishing the BPAs, the procedures in (a)(2) above must be followed. The procedures at (a)(2) do not apply to orders issued under multiple BPAs. Authorized users must transmit the request for quote for an order to all BPA holders and then place the order with the Schedule contractor that represents the best value.

(2) Review BPAs Periodically: Such reviews shall be conducted at least annually. The purpose of the review is to determine whether the BPA still represents the best value. (See FAR 8.404)

c. The ordering activity should give preference to small business concerns when two or more contractors can provide the services at the same firm-fixed price or ceiling price.

d. When the ordering activity's requirement involves both products as well as executive, administrative and/or professional, services, the ordering activity should total the prices for the products and the firm-fixed price for the services and select the contractor that represents the best value. (See FAR 8.404)

e. The ordering activity, at a minimum, should document orders by identifying the contractor from which the services were purchased, the services purchased, and the amount paid. If other than a firm-fixed price order is placed, such documentation should include the basis for the determination to use a labor-hour or time-and-materials order. For ordering activity requirements in excess of the micro-purchase threshold, the order file should document the evaluation of Schedule contractors' quotes that formed the basis for the selection of the contractor that received the order and the rationale for any trade-offs made in making the selection.

4. ORDER

a. Agencies may use written orders, EDI orders, blanket purchase agreements, individual purchase orders, or task orders for ordering services under this contract. Blanket Purchase Agreements shall not extend beyond the end of the contract period; all services and delivery shall be made and the contract terms and conditions shall continue in effect until the completion of the order. Orders for tasks which extend beyond the fiscal year for which funds are available shall include FAR 52.232-19 (Deviation – May 2003) Availability of Funds for the Next Fiscal Year. The purchase order shall specify the availability of funds and the period for which funds are available.

b. All task orders are subject to the terms and conditions of the contract. In the event of conflict between a task order and the contract, the contract will take precedence.

5. PERFORMANCE OF SERVICES

a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.

b. The Contractor agrees to render services only during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.

c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.

d. Any Contractor travel required in the performance of IT/EC Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts.

6. STOP-WORK ORDER (FAR 52.242-15) (AUG 1989)

a. The Contracting Officer may, at any time, by written order to the Contractor, require the Contractor to stop all, or any part, of the work called for by this contract for a period of 90 days after the order is delivered to the Contractor, and for any further period to which the parties may agree. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Within a period of 90 days after a stop-work is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either-

(1) Cancel the stop-work order; or

(2) Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this contract.

b. If a stop-work order issued under this clause is canceled or the period of the order or any extension thereof expires, the Contractor shall resume work. The Contracting Officer shall make an equitable adjustment in the delivery schedule or contract price, or both, and the contract shall be modified, in writing, accordingly, if-

(1) The stop-work order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this contract; and

(2) The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided, that, if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon the claim submitted at any time before final payment under this contract.

c. If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.

d. If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.

7. INSPECTION OF SERVICES

The Inspection of Services–Fixed Price (AUG 1996) (Deviation – May 2003) clause at FAR 52.246-4 applies to firm-fixed price orders placed under this contract. The Inspection–Time-and-Materials and Labor-Hour (JAN 1986) (Deviation – May 2003) clause at FAR 52.246-6 applies to time-and-materials and labor-hour orders placed under this contract.

8. RESPONSIBILITIES OF THE CONTRACTOR

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227-14 (Deviation – May 2003) Rights in Data – General, may apply.

9. RESPONSIBILITIES OF THE ORDERING ACTIVITY

Subject to security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite IT/EC Services.

10. INDEPENDENT CONTRACTOR

All IT/EC Services performed by the Contractor under the terms of this contract shall be as an independent Contractor, and not as an agent or employee of the ordering activity.

11. ORGANIZATIONAL CONFLICTS OF INTEREST

a. Definitions.

“Contractor” means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party to this contract.

“Contractor and its affiliates” and “Contractor or its affiliates” refers to the Contractor, its chief executives, directors, officers, subsidiaries, affiliates, subcontractors at any tier, and consultants and any joint venture involving the Contractor, any entity into or with which the Contractor subsequently merges or affiliates, or any other successor or assignee of the Contractor.

An “Organizational conflict of interest” exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on ordering activities by the Contractor and its affiliates, may either (i) result in an unfair competitive advantage to the Contractor or its affiliates or (ii) impair the Contractor’s or its affiliates’ objectivity in performing contract work.

b. To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the ordering activity, ordering activities may place restrictions on the Contractors, its affiliates, chief executives, directors, subsidiaries and subcontractors at any tier when placing orders against schedule contracts. Such restrictions shall be consistent with FAR 9.505 and shall be designed to avoid, neutralize, or mitigate organizational conflicts of interest that might otherwise exist in situations related to individual orders placed against the schedule contract. Examples of situations, which may require restrictions, are provided at FAR 9.508.

12. INVOICES

The Contractor, upon completion of the work ordered, shall submit invoices for IT/EC services. Progress payments may be authorized by the ordering activity on individual orders if appropriate. Progress payments shall be based upon completion of defined milestones or interim products. Invoices shall be submitted monthly for recurring services performed during the preceding month.

13. PAYMENTS

For firm-fixed price orders the ordering activity shall pay the Contractor, upon submission of proper invoices or vouchers, the prices stipulated in this contract for service rendered and accepted. Progress payments shall be made only when authorized by the order. For time-and-materials orders, the Payments under Time-and-Materials and Labor-Hour Contracts at FAR 52.232-7 (DEC 2002), (Alternate II – Feb 2002) (Deviation – May 2003) applies to time-and-materials orders placed under this contract. For labor-hour orders, the Payment under Time-and-Materials and Labor-Hour Contracts at FAR 52.232-7 (DEC 2002), (Alternate II – Feb 2002) (Deviation – May 2003)) applies to labor-hour orders placed under this contract.

14. RESUMES

Resumes shall be provided to the GSA Contracting Officer or the user ordering activity upon request.

15. INCIDENTAL SUPPORT COSTS

Incidental support costs are available outside the scope of this contract. The costs will be negotiated separately with the ordering activity in accordance with the guidelines set forth in the FAR.

16. APPROVAL OF SUBCONTRACTS

The ordering activity may require that the Contractor receive, from the ordering activity's Contracting Officer, written consent before placing any subcontract for furnishing any of the work called for in a task order.

17. DESCRIPTION OF IT SERVICES AND PRICING

Job Title: Program Manager

Minimum/General Experience: Extensive years of management experience throughout a project management life cycle and delivery of state-of-the-art technology solutions. Includes coordinating work activity, allocation of resources, managing performance, and development of solutions for Information Technology challenges. Specialized experience in the technologies that meet the specific statement of work for the services to be provided may be substituted for years of experience.

Functional Responsibility: Responsible for project management in accordance with client requirements and organizational guidelines. Specific duties may include oversight of program level cost, schedule, performance and deliverable services as well as products. Detects and analytically solves a wide variety of business problems. Provides the strategic planning for successful project completion. Directs, organizes and monitors work activity and is responsible for meeting program cost, schedule and performance objectives. Provides overall managerial direction for multiple projects. Formulates and reviews project feasibility studies, determines cost and ensures conformance to quality standards.

Minimum Education: Masters degree or specialized experience in the technologies that meet the specific statement of work for the services to be provided may be substituted for years of experience. Bachelor’s degree with ten+ years of experience.

Job Title: Project Manager

Minimum/General Experience: Experience managing large-scale, high-quality, state-of-the-art Information Technology (IT) projects. Experience in managing the business issues associated with client requirements.

Functional Responsibility: Manages the day-to-day operations of the IT project. Prepares project estimates and workplans using company experience on prior engagements and the company methods and tools for planning and estimating projects. Prepares and presents project status reports to the company and the client. Resolves IT project staffing and planning issues. Works with client resources on issues in implementing the IT project. Manages the company IT staff assigned to the project. Works with the Program Manager to resolve staffing and company resource issues. Conducts preliminary quality assurance over IT project deliverables (interim and key) and technology project activities.

Minimum Education: Masters degree or specialized experience in the technologies that meet the specific statement of work for the services to be provided may be substituted for years of experience. Bachelor’s degree with five+ years of experience.

Job Title: Network Analyst II

Minimum/General Experience: Ten years experience in LAN/WAN/MAN Infrastructure, in protocol analysis and knowledge of Open System Interconnect (OSI) protocols, particularly Transport Control Protocol/Internet Protocol (TCP/IP), X.25, X.400, and X.500. Also requires experience with Asynchronous Transfer Mode (ATM), frame relay, bridges, routers, gateways, FDDI, and UNIX/Linux operating systems. In addition, this position requires experience as a Certified Network Engineer (CNE) or Master CNE. Furthermore, this position necessitates specialized experience supervising the operation and maintenance of communication network systems, which may be mainframe, mini, or client/server based, planning, installation, and support. Also requires five years experience managing services and personnel. General experience must include operations experience on a large-scale computer system or a multi-server LAN. The Network Analyst II must have experience supervising and leading staff and have a demonstrated ability to communicate orally and in writing.

Functional Responsibility: The Network Analyst II evaluates communication hardware and software, troubleshoots LAN/WAN and other network related problems, and provides technical expertise for performance and configuration of networks. The Network Analyst II shall perform general LAN/WAN administration and provide technical leadership in the integration and testing of complex large-scale computer integrated networks. Also, the Network Analyst II shall design and optimize network topologies, optimize system operation and resource utilization, and perform system capacity analysis and planning. In addition, the Network Analyst II shall be knowledgeable of IT security issues and help ensure that there is a secure IT environment. Furthermore, the Network Analyst II shall provide assistance to users in accessing and using IT systems. Moreover, the Network Analyst II shall schedule conversions and supervise maintenance of systems. Additionally, the Network Analyst II shall coordinate IT issues with the necessary people at various sites.

Minimum Education: A Bachelor's degree in Computer Science, Information Systems, Engineering, Business, or other related disciplines is required. An engineering degree or related engineering work, mainly in the fields of civil or mechanical engineering, would be preferred. Associates degree with ten+ years in related field.

Job Title: Network Analyst I

Minimum/General Experience: Five or more years of experience analyzing LAN/WAN/MAN network hardware and software. Requires competence analyzing network characteristics (e.g. traffic, connect time, transmission speeds, packet sizes, and throughput) and recommends procurement, upgrades, removals and other modifications to network components. Also requires specialized knowledge of PC operating systems, e.g., DOS, Windows, etc., as well as specialized experience in networking, mail standards.

Functional Responsibility: The Network Analyst I assists the Network Analyst II in maintaining large LAN systems. The Network Analyst I also helps support a WAN system using TCP/IP, which includes connectivity to mainframes. In addition, the Network Analyst I conducts site surveys and assesses and documents current site network configuration and user requirements. Furthermore, the Network Analyst I shall follow engineering plans and site installation Technical Design Packages. Moreover, the Network Analyst I shall develop installation schedules and assist in the preparation of drawing and documenting configuration changes. Additionally, the Network Analyst I shall prepare site installation and test reports and coordinate and perform installation of equipment and workstations. The Network Analyst I’s other duties include providing technical and software support to end-users; serving as the initial point of contact for troubleshooting hardware/software PC and printer problems; and providing phone and in-person support to users in the areas of e-mail, directories, standard Windows desktop applications, and applications developed under this contract or developed prior to the commencement of this contract. Also, the Network Analyst I is responsible for installing, maintaining, and upgrading computer workstations and software. In addition, the Network Analyst I shall provide technical assistance and training; perform evaluations of computer hardware and software; and serve as a liaison with vendors for new hardware/software purchases.

Minimum Education: Bachelors Degree in Computer Sciences or related field. Associates degree with five+ years in related field.

Job Title: Network Technician II

Minimum/General Experience: Six years experience directly related in the implementation and maintenance of local and wide area network application systems; or completion of a job-training program in networks or data communications certified by Novell, Microsoft.

Functional Responsibility: Specialized subject matter expertise in the operation of network systems including LANs and WANs. A Network Technician II provides general direction. Responsibilities do not include direct supervision of other positions but may serve as lead workers. Excellent knowledge of overall networking technologies; levels of technologies; test/diagnostic tools; and extensive trouble shooting abilities.

Minimum Education: A Bachelor s degree in computer science, engineering, mathematics, or related field, with 2 years experience, or equivalent. Associates degree with five+ years experience in related field.

Job Title: Network Technician I

Minimum/General Experience: Four years experience directly related in the implementation and maintenance of local and wide area network application systems; or completion of a job training program in networks or data communications certified by Novell, Microsoft.

Functional Responsibility: Specialized subject matter expertise in the operation of network systems including LANs and WANs. A Network Technician II provides general direction. Responsibilities do not include direct supervision of other positions but may serve as lead workers. Excellent knowledge of overall networking technologies; levels of technologies; test/diagnostic tools; and extensive trouble shooting abilities.

Minimum Education: A Bachelor's degree in computer science, engineering, mathematics, or related field, with one year experience, or equivalent. Associates' degree with three+ years of experience in related field.

Job Title: Telecommunications Engineer II

Minimum/General Experience: This senior level IT professional has the ability to analyze, design and implement communications networks for data, voice and video applications. Will have expertise in communications protocols, industry standards, and communications equipment provided by various vendors. Will be abreast of industry standards, codes, regulations and legislative initiatives in the field. Six years of applicable professional experience. An advanced degree is equivalent to 3 years of experience.

Functional Responsibility: Will analyze existing client network architectures to make recommendations for improvement. Will lead design efforts for medium to large new communication networks using client specifications for performance, dependability and scalability. Will stay current with industry standards, codes and regulations. Will remain current with emerging technologies in the communications field. Will provide white papers and/or informational reports at the request of company or client management. Will direct the work of less senior company staff and provide guidance and mentoring to less senior network consultants.

Minimum Education: Bachelor's Degree or equivalent professional experience. One or more certifications in the communications field are required. Associates degree with five+ years experience in related field.

Job Title: Telecommunications Engineer I

Minimum/General Experience: This senior level IT professional has the ability to analyze, design and implement communications networks for data, voice and video applications. Will have expertise in communications protocols, industry standards, and communications equipment provided by various vendors. Will be abreast of industry standards, codes, regulations and legislative initiatives in the field. Three years of applicable professional experience. An advanced degree is equivalent to 3 years of experience.

Functional Responsibility: Will analyze existing client network architectures to make recommendations for improvement. Will lead design efforts for small to medium new communication networks using client specifications for performance, dependability and scalability. Will stay current with industry standards, codes and regulations. Will remain current with emerging technologies in the communications field. Will direct less senior company staff under the guidance of a senior consultant.

Minimum Education: Bachelor's Degree or equivalent professional experience. One or more certifications in the communications field are desirable but not required. Associates degree with three+ years experience in related field.

Job Title: Telecommunications Technician II

Minimum/General Experience: Comprehensive problem solving and customer support experience.

Functional Responsibility: Lead telecommunications technician providing over site and customer support for staging, installation and programming of various voice and data systems and video technology. Excellent knowledge of voice/data switching and routing technologies.

Minimum Education: Bachelor's Degree or equivalent professional experience. One or more certifications in the communications field are desirable but not required. Associates degree with five+ years experience in related field.

Job Title: Telecommunications Technician I

Minimum/General Experience: Extensive problem solving and customer support abilities.

Functional Responsibility: Experienced technician providing staging, installation and programming for various voice and data systems and video technology. Excellent knowledge of voice/data switching and routing technologies.

Minimum Education: Bachelor's Degree or equivalent professional experience. One or more certifications in the communications field are desirable but not required. Associates degree with five+ years experience in related field.

Job Title: Technical Writer

Minimum/General Experience: Experience in creating user and/or systems manuals or documentation using input from senior level consultants. Will have expertise in word processing and desktop publishing software. Two to four years of applicable professional experience. An Associate's Degree is equivalent to one year experience. A Bachelor's Degree is equivalent to 3 years of experience

Functional Responsibility: Will create user and/or system manuals or documentation using input from senior level consultant and placed in a format that satisfies client specifications.

Minimum Education: Graduation from High School or equivalent.

Job Title: Technician II

Minimum/General Experience: Excellent knowledge of a wide variety of communication and information technology and troubleshooting methodology.

Functional Responsibility: Lead technician for field configuration, burn-in, set-up, diagnostic performance and troubleshooting of equipment. Provides oversight for configuration, burn-in, set-up, diagnostic performance and troubleshooting of various kinds of equipment in WWT integration laboratory prior to delivery to customer.

Minimum Education: High-School Diploma, or Microsoft Certified Product Specialist (MCP) Certification or equivalent.

Job Title: Technician I

Minimum/General Experience: Excellent knowledge of a wide variety of communication and information technology and troubleshooting methodology.

Functional Responsibility: Experienced technician for configuration, burn-in, set-up, diagnostic performance and troubleshooting of various kinds of equipment in the field or in the WWT integration laboratory prior to delivery to customer.

Minimum Education: High-School Diploma or equivalent.

Job Title: Senior Software Engineer

Minimum/General Experience: This senior level IT professional has the ability to analyze, design and implement computer programs for all applications. Will have expertise in various computer languages, industry standards, and computer operating systems and equipment provided by various vendors. Will be abreast of industry standards, codes, regulations and legislative initiatives in the field. Six years of applicable professional experience. An advanced degree is equivalent to 3 years of experience.

Functional Responsibility: Will analyze existing client software architectures to make recommendations for improvement. Will lead design efforts for medium to large new software projects using client specifications for performance, dependability and scalability. Will stay current with industry standards, codes and regulations. Will remain current with emerging technologies in the computer software field. Will provide white papers and/or informational reports at the request of company or client management. Will direct the work of less senior company staff and provide guidance and mentoring to less senior consultants.

Minimum Education: Bachelor’s Degree. One or more certifications in computer software languages are required

---

Job Title: Software Engineer

Minimum/General Experience: This senior level IT professional has the ability to analyze, design and implement computer software applications. Will have expertise in protocols, industry standards, and operating systems provided by vendors. Be abreast of industry standards, codes, regulations and legislative initiatives in the field. Three years of applicable professional experience. An advanced degree is equivalent to 3 years of experience.

Functional Responsibility: Will analyze existing client network architectures to make recommendations for improvement. Will lead design efforts for small to medium new software systems. Will stay current with industry standards, codes and regulations. Will remain current with emerging technologies in the computer field. Will direct company staff under the guidance of a senior consultant.

Minimum Education: Bachelor’s Degree or equivalent professional experience. One or more certifications in the communications field are desirable but not required. Associates degree with three+ years experience in related field.

Labor Category	**Hourly Rate**
Program Manager	$ 182
Project Manager	$ 167
Network Analyst II	$ 167
Network Analyst I	$ 130
Senior Software Engineer	$ 150
Software Engineer	$ 130
Network Technician I	$ 78
Telecommunications Engineer II	$ 167
Telecommunications Engineer I	$ 130
Telecommunications Technician II	$ 105
Telecommunications Technician I	$ 78
Technical Writer	$ 63
Technician II	$ 52
Technician I	$ 40

USA COMMITMENT TO PROMOTE SMALL BUSINESS PARTICIPATION PROCUREMENT PROGRAMS

PREAMBLE

Cityroots, Inc. provides commercial products and services to ordering activities. We are committed to promoting participation of small, small disadvantaged and women-owned small businesses in our contracts. We pledge to provide opportunities to the small business community through reselling opportunities, mentor-protégé programs, joint ventures, teaming arrangements, and subcontracting.

COMMITMENT

To actively seek and partner with small businesses.

To identify, qualify, mentor and develop small, small disadvantaged and women-owned small businesses by purchasing from these businesses whenever practical.

To develop and promote company policy initiatives that demonstrate our support for awarding contracts and subcontracts to small business concerns.

To undertake significant efforts to determine the potential of small, small disadvantaged and women-owned small business to supply products and services to our company.

To insure procurement opportunities are designed to permit the maximum possible participation of small, small disadvantaged, and women-owned small businesses.

To attend business opportunity workshops, minority business enterprise seminars, trade fairs, procurement conferences, etc., to identify and increase small businesses with whom to partner.

To publicize in our marketing publications our interest in meeting small businesses that may be interested in subcontracting opportunities.

We signify our commitment to work in partnership with small, small disadvantaged and women-owned small businesses to promote and increase their participation in ordering activity contracts. To accelerate potential opportunities please contact Deborah Ramirez-Tinoco at (661) 588-0639 or (661) 589-8849 or by email at deb@cityroots.com.

BEST VALUE
BLANKET PURCHASE AGREEMENT
FEDERAL SUPPLY SCHEDULE

Cityroots, Inc.

In the spirit of the Federal Acquisition Streamlining Act (ordering activity) and (Contractor) enter into a cooperative agreement to further reduce the administrative costs of acquiring commercial items from the General Services Administration (GSA) Federal Supply Schedule Contract(s) ____________________.

Federal Supply Schedule contract BPAs eliminate contracting and open market costs such as: search for sources; the development of technical documents, solicitations and the evaluation of offers. Teaming Arrangements are permitted with Federal Supply Schedule Contractors in accordance with Federal Acquisition Regulation (FAR) 9.6.

This BPA will further decrease costs, reduce paperwork, and save time by eliminating the need for repetitive, individual purchases from the schedule contract. The end result is to create a purchasing mechanism for the ordering activity that works better and costs less.

Signatures

___________________________________ ___________________________________
Ordering Activity Date Contractor Date

BPA NUMBER_____________

(CUSTOMER NAME)
BLANKET PURCHASE AGREEMENT

Pursuant to GSA Federal Supply Schedule Contract Number(s)____________, Blanket Purchase Agreements, the Contractor agrees to the following terms of a Blanket Purchase Agreement (BPA) EXCLUSIVELY WITH (ordering activity):

(1) The following contract items can be ordered under this BPA. All orders placed against this BPA are subject to the terms and conditions of the contract, except as noted below:

MODEL NUMBER/PART NUMBER	*SPECIAL BPA DISCOUNT/PRICE
______________________________	______________________________
______________________________	______________________________
______________________________	______________________________

(2) Delivery:

DESTINATION	DELIVERY SCHEDULES / DATES
______________________________	______________________________
______________________________	______________________________
______________________________	______________________________

(3) The ordering activity estimates, but does not guarantee, that the volume of purchases through this agreement will be _________________________.

(4) This BPA does not obligate any funds.

(5) This BPA expires on _________________ or at the end of the contract period, whichever is earlier.

(6) The following office(s) is hereby authorized to place orders under this BPA:

OFFICE	POINT OF CONTACT
______________________________	______________________________
______________________________	______________________________
______________________________	______________________________

(7) Orders will be placed against this BPA via Electronic Data Interchange (EDI), FAX, or paper.

(8) Unless otherwise agreed to, all deliveries under this BPA must be accompanied by delivery tickets or sales slips that must contain the following information as a minimum:

(a) Name of Contractor;

(b) Contract Number;

(c) BPA Number;

(d) Model Number or National Stock Number (NSN);

(e) Purchase Order Number;

(f) Date of Purchase;

(g) Quantity, Unit Price, and Extension of Each Item (unit prices and extensions need not be shown when incompatible with the use of automated systems; provided, that the invoice is itemized to show the information); and

(h) Date of Shipment.

(9) The requirements of a proper invoice are specified in the Federal Supply Schedule contract. Invoices will be submitted to the address specified within the purchase order transmission issued against this BPA.

(10) The terms and conditions included in this BPA apply to all purchases made pursuant to it. In the event of an inconsistency between the provisions of this BPA and the Contractor's invoice, the provisions of this BPA will take precedence.

****

BASIC GUIDELINES FOR USING
"CONTRACTOR TEAM ARRANGEMENTS"

Federal Supply Schedule Contractors may use "Contractor Team Arrangements" (see FAR 9.6) to provide solutions when responding to an ordering activity requirements.

These Team Arrangements can be included under a Blanket Purchase Agreement (BPA). BPAs are permitted under all Federal Supply Schedule contracts.

Orders under a Team Arrangement are subject to terms and conditions or the Federal Supply Schedule Contract.

Participation in a Team Arrangement is limited to Federal Supply Schedule Contractors.

Customers should refer to FAR 9.6 for specific details on Team Arrangements.

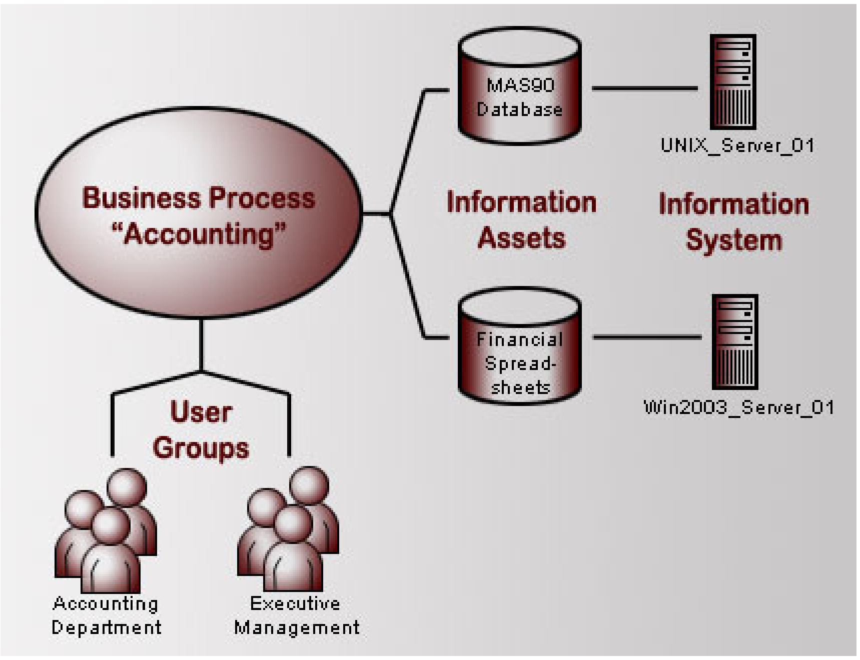
Here is a general outline on how it works:

- The customer identifies their requirements.
- Federal Supply Schedule Contractors may individually meet the customers needs, or -
- Federal Supply Schedule Contractors may individually submit a Schedules "Team Solution" to meet the customer's requirement.
- Customers make a best value selection.

ECM SOFTWARE DESCRIPTIVE INFORMATION

Security Associates Corp™ has taken the next step in proactive risk assessment compliance management by developing its industry-leading product **Enterprise Compliance Manager™** (**ECM™**) into a web-based compliance and accreditation solution. This artificial intelligence system allows organizations to assess risk, prioritize vulnerabilities, and evaluate policies against applicable standards for regulatory compliance.

The decision support system allows users to identify business processes, then categorize and assign value to information assets that belong to those business processes. Once identified, the system then maps this data back to existing standards to measure compliance. These business processes or standards can then be further associated to physical assets or even polices within an organization. The DSS weights assets against specific questions to determine predefined consequences based on out of compliance responses.



How information is gathered

ECM™ allows users to create an encrypted session into their profile to answer questions specific to their respective department or business unit within an organization. Security profiles are configured to allow various levels of access to data based on classification and privilege level of the end user.

One of the ways the system saves time is by reducing the amount of effort required to complete the interview process by utilizing a relational database function that facilitates populating all fields within the DSS from predefined occupational spreadsheets. Access controls allow managers to review questionnaires for completeness prior to final submission. Test conditions can be executed against all network assets, applications and polices using the broadest suite of tools on the market today. Methods for measuring these include:

- Network based assessments
- Host based assessments
- Application based assessments
- Security policy assessments
- Business policy assessments
- Compliance and certification assessments

Interoperability

In addition to incorporating its own scanning products, **ECM™** also interoperates with legacy asset management solutions, application scanning solutions, host based scanning products, and network based scanning products. By leveraging what the customer has already acquired, **ECM™** reduces the cost of technology ownership.

Policy Assessments

Policy assessments are a tedious task requiring experienced consultants and compliance managers with years of industry experience in vulnerability assessments and regulatory compliance. With ECM's policy assessment engine you plug in your existing policies, answer required questions and receive complete datasheets on out of compliance issues or industry updates. Not only does ECM identify out of compliance remediation plans it also provides actual policies. There is also a policy enforcement module available.

Automated reporting & customization

Reporting with **ECM™** is performed by identifying and prioritizing all out of compliance conditions. Once identified these conditions are prioritized based on a ranking system created by each business unit leader or stakeholder. By allowing the manager to identify and rank business processes and information asset associations, vulnerabilities and out of compliance conditions receive the most accurate ranking according to the organization. Where standards take precedence, these findings can supercede organizational rankings depending on the type of report requested from the system.

With a customizable configuration wizard, privileged users can create and update industry standards, questions, consequences, and even modify policies in real-time. With over 10, 000 questions amongst three databases within the DSS, users can be assured they have the most comprehensive assessment solutions on the market today.

Methodology

Security Associates Corp™ provides a "Vulnerabilities Assessment" which is a more holistic approach to evaluating information systems security. These proprietary processes and procedures provide a comprehensive, in depth look into your information systems. The goal is to document your Information systems ability to protect your information assets confidentiality, integrity and availability.

ECM's automated security assessment process evaluates 15 major parameters of organizations. These parameters include:

- Administrative policies and procedures
- Roles and Responsibilities
- Authorization and identification

- Virus Controls
- Audit
- Configuration management
- Application security
- Data Classification
- User workstation security
- Server / host security
- Network security
- Perimeter security
- Telecommunications security
- Physical plant security
- Existing contingency and crisis planning

While it's not uncommon for a manager to select a safeguard without first doing a risk analysis, the result may be a serious over-expenditure of funds for protective measures that lead to a false sense of security. The Assessment software bridges the communication gap between the IT staff and the economic decision maker. This is accomplished by providing a Return on Investment (ROI) analysis prioritizing the most significant security risks and identifying where to best allocate budgetary funding (Do we help determine a dollar amount for remediation to the out of compliance issue?).

Quarterly risk assessments are an essential part of conducting business in today's environment. Whether compelled by good security practices, government requirements, institutional oversight, or stockholder protection, comprehensive vulnerability assessments are an essential part of an organizations protection strategy. The vulnerabilities assessment will identify your business' vulnerabilities, help mitigate your risk, and define implementation measures to aid in the best allocation of your security budget. The assessment will assist an organization in developing a complete understanding of their security environment, thus allowing the business to focus on their core competencies.

The Assessment Process

Step 1. The Pre-Assessment Phase

In this phase, the user will access multiple forms and databases to ensure easy tracking of all logistics needed to administrate a comprehensive security assessment. The databases include the ability to:

- Identify the customer's priorities.
- Chronicle the actions of the assessors.
- Use the Pre-Assessment Checklist to track everything needed before an assessment.
- Determine and track customer interview schedules.
- Identify customer objectives.
- Track business functions to IT functions.
- Track all business process stakeholders.
- Set up and track appropriate interview questions and answers.

- Track all meeting times, dates, and conversations.
- Map the assessment objectives back to the statement of work.
- Ensure that multiple assessors are accomplishing their objectives.

Step 2. Actual-Assessment Phase

The system allows the user to perform the following critical risk assessment functions seamlessly, either separately or in tandem:

- Utilize industry-accepted vulnerability scanning tools to import data into the Assessment software, which will identify anomalies and errors (ISS-Security Scanner, CyberCop support today). The system also gives the flexibility to use on board scanners
- “Health check” capability for quick overview of security risk status. Answer fewer questions to determine overall security risk within physical, operational and network areas. (Increase assessor productivity and reduce costs)
- The questionnaire function allows you to easily pare down the list of questions to ensure that you only ask those that are required, while redundant and non-related questions are skipped.
- The Reference database will dynamically locate and access key system commands and port information back into the tool.
- The modular architecture designed with the questionnaire, allows the assessor to drill deeper into business processes and identify risk.

Core assessment areas include:

- Physical Security
- Network Security
- Operational Security
- Policy compliance
- Application Security

Templates are available for the following assessments:

- Sarbanes Oxley
- HIPAA Compliance
- Gramm, Leach, Bliley Act
- ISO17799
- Federal Energy Regulatory Committee
- Federal Information Security Management Act
- Department Of Defense Information Technology Security Certification and Accreditation Program
- NIST 800-53 DIACAP

Step 3. Post-Assessment Phase

Report generation is performed during the Post-assessment. In most cases consultants spend a majority of their time having to reformat various sources of information into a final report for submission. With our template builder, the assessor will quickly create custom reports from one of our default report templates. Our methodology bridges the gap between the IT staff and the business stakeholder by providing associations of assets and protection analysis, a prioritization of the most significant security risks, and vulnerabilities. Our methodology and tool provides the ability to:

- Provide three default reports: Executive Summary, Managers & Technical Report, detailed report, and appendices.
- Provide detailed and comprehensive reports on assessment results, identify security vulnerabilities, and suggest potential solutions for these vulnerabilities.
- Rank potential risk in various areas including, but not limited to: IDS, perimeter, physical, and email security, encryption, privacy, policy and procedures, employee security training, etc.
- Calculate security solution implementation levels of exposure including, but not limited to: installation, configuration, penetration tests, maintenance and monitoring.
- Recommend fixes for reducing security weaknesses.
- Allow the consultant to create specific questions regarding their environment with ease.

Product Code	Product Name	SIN	Price
ECMQSP01 (5 Users)	**Enterprise Compliance ManagerSA™ (ECM™) – Quick Start Package L1** One Server license required for one location Document Management; Workflow Management; Scanner Set-up option; Single-site support; One administrative key; 5 User keys; One template.		
	One Template	132-34	$7,840
	Annual User License Fee	132-32	$783
	Annual Server License Fee (One server)	132-32	$11,760
	Onsite installation includes initial application configuration & training	132-34	$3,920
	Quick Start Package L1 – Total Price		**$24,303**
ECMSAL1 (1-10 Users)	**Enterprise Compliance ManagerSA™ (ECM™) – Small Business Level 1** One Server license required for one location E-Records Management; Workflow Management; Scanner Set-up option; Single-site support; One administrative keys; up to 10 User keys; One template.		
	Additional Templates	132-34	$10,000
	Annual Maintenance	132-34	$6,250
	Annual User License Fee ($100 per user for 10 users)	132-32	$1,000
	Annual Server License Fee (One server)	132-32	$20,000
	Onsite installation includes initial application configuration	132-34	$5,000
	User Training	132-50	$4,040
	Small Business – Level 1 Total Price (includes one template)		**$36,290**

Product Code	Product Name	SIN	Price
ECMSAL2 (11-25 Users)	**Enterprise Compliance ManagerSA™ (ECM™) – Small Business Level 2** One Server license required for one location E-Records Management; Workflow Management; Scanner Set-up option; Single-site support; One administrative keys; up to 25 User keys; One template.		
	Additional Templates	132-34	$10,000
	Annual Maintenance	132-34	$15,000
	Annual User License Fee ($100 per user for 25 users)	132-32	$2,500
	Annual Server License Fee (One server)	132-32	$40,000
	Onsite installation includes initial application configuration	132-34	$7,500
	User Training	132-50	$4,040
	Small Business – Level 2 Total Price (includes one template)		**$69,040**
ECML2 (25-50 Users)	**Enterprise Compliance Manager™ (ECM™) - Level 2** One Server license required for one location E-Records Management; Workflow Management; Scanner Set-up option; Single-site support; 1 to 5 administrative keys; up to 50 User keys; One template.		
	Additional Templates	132-34	$15,000
	Annual Maintenance	132-34	$15,200
	Annual User License Fee ($100 per user for 50 users)	132-32	$5,000
	Annual Server License Fee (One server)	132-32	$70,000
	Onsite installation includes initial application configuration	132-34	$9,500
	User Training	132-50	$4,040
	Level 2 Total Price (includes one template)		**$103,740**

Product Code	Product Name	SIN	Price
ECML3 (51-250 Users)	**Enterprise Compliance Manager™ (ECM™) - Level 3** Three Server licenses required for three locations E-Records Management; Workflow Management; Scanner Set-up option; Single-site support; 1 to 5 administrative keys; up to 250 User keys; One template		
	Additional Templates	132-34	$15,000
	Annual Maintenance	132-34	$22,140
	Annual User License Fee ($69 per user for 250 users)	132-32	$17,250
	Annual Server License Fee (One server)	132-32	$90,000
	Onsite installation includes initial application configuration	132-34	$12,500
	User Training	132-50	$7,878
	Level 3 Total Price (includes one template)		**$149,768**
ECML4 (251- 500 Users)	**Enterprise Compliance Manager™ (ECM™)** **Level 4 - Medium Business Solution** Seven Server licenses required for seven locations E-Records Management; Workflow Management; Scanner Set-up option; Seven-site support; 5 to 10 administrative keys; up to 500 User keys		
	Additional Templates	132-34	$15,000
	Annual Maintenance	132-34	$42,962
	Annual User License Fee ($59 per user for 500 users)	132-32	$29,500
	Annual Server License Fee (Three servers)	132-32	$180,000
	Onsite installation includes initial application configuration	132-34	$17,000
	User Training	132-50	$9,310
	Level 4 Total Price (includes one template)		**$278,772**

Product Code	Product Name	SIN	Price
ECML5 (501-1,000 Users)	**Enterprise Compliance Manager™ (ECM™)** **Level 5 - Large Business Solution** 10 Server licenses required for up to 10 location E-Records Management; Workflow Management; Scanner Set-up option; Ten-site support; 10 to 15 administrative keys; 1,000 User keys		
	Additional Templates	132-34	$15,000
	Annual Maintenance	132-34	$49,360
	Annual User License Fee ($39 per user for 1,000 users)	132-32	$39,000
	Annual Server License Fee (Five servers)	132-32	$200,000
	Onsite installation includes initial application configuration	132-34	$22,000
	User Training	132-50	$12,800
	Level 5 Total Price (includes one template)		**$323,160**
ECML6 (1,001- 2,500 Users)	**Enterprise Compliance Manager™ (ECM™)** **Level 6 - Enterprise Business Solution** 15 Server licenses required for up to 15 locations E-Records Management; Workflow Management; Scanner Set-up option; Fifteen-site support for integrated solution; 25 administrative keys; up to 2,500 User keys		
	Additional Templates	132-34	$15,000
	Annual Maintenance	132-34	$88,965
	Annual User License Fee ($29 per user for 2,500 users)	132-32	$72,500
	Annual Server License Fee (Twelve servers)	132-32	$360,000
	Onsite installation includes initial application configuration	132-34	$35,000
	User Training	132-50	$17,325
	Level 6 Total Price (includes one template)		**$573,790**

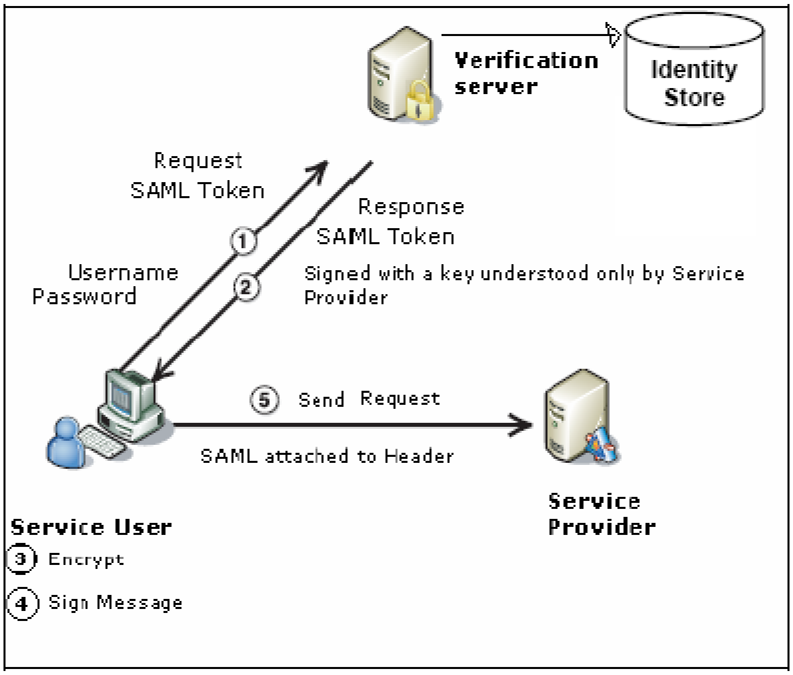
Product Code	Product Name	SIN	Price
ECML7 (2,501- 5,000 Users)	**Enterprise Compliance Manager™ (ECM™)** **Level 7 - Enterprise Small Global Option** 30 Server Licenses required for up to 30 locations E-Records Management; Workflow Management; Scanner Set-up option; Thirty-site support for integrated solution; 50 administrative keys; up to 5,000 User keys		
	Additional Templates	132-34	$15,000
	Annual Maintenance	132-34	$192,000
	Annual User License Fee ($22 per user for 5,000 users)	132-32	$110,000
	Annual Server License Fee (Twenty-five servers)	132-32	$850,000
	Onsite installation includes initial application configuration	132-34	$50,000
	User Training	132-50	$22,500
	Level 7 Total Price (includes one template)		**$1,224,500**

Validate and Authorize Transactions via the Compliance Authorization Gateway

SECURITY ASSOCIATES CORP.

Introduction

As the publications and news reports continue to grow regarding website hacks, database breaches and computer hard drive compromises, never has a time been greater for authorized transaction solutions. The fact that once someone has inside access to a system or database does not have to mean that information can be compromised. With Transaction Authorization Gateways the rules are the same, if you cannot prove you are the authorized party attempting to access information, you will not be authorized to do so, more importantly the moment an unauthorized attempt is made on your critical resources your administrator will or designated authority be notified of the activity.



Simple Transaction Process

Financial Services Transactions

As the Financial Services industry begins to develop higher-level value-added services around B2B business applications, the critical foundation of these services will include secure services that must ensure acceptable levels of identity, data confidentiality, authentication, and transaction authorization. Security Associates Corporation (SAC) is working within the Financial Services industry, to provide these required services. SAC targeted applications that integrate with the SAC Authorization Gateway service to provide authentication and authorization between users within the organization and in Electronic Data Interchange (EDI) transactions, CRM, EDP applications.

Health Care Transactions

Healthcare organizations that must adhere to HIPAA requirements need an Electronic Data Interchange transaction management and analysis software solution for processing, monitoring, storing, reporting and analyzing electronic transaction data within their environments. These software solutions must use gateway solutions to meet the needs of current and potential new customers. These software solutions must beable to track and audit the flow of HIPAA data, monitor patterns and variability within the business transactions and establish triggers and alerts for exception handling. The SAC Authorization Gateway addresses these issues in addition to providing the following capabilities:

- Reduce the incidence of lost or misplaced data
- Improve transactional data quality
- Increase first pass transaction acceptance rates with payers which directly impacts revenue cycle metrics and revenue stream
- Improve providers ability to identify payer adjudication anomalies

The SAC Authorization Gateway can be installed in health care organizations (HCO), to be deployed throughout an HCO's network and supply chain environment, to address the authentication requirements in HIPAA. The Authorization Gateway can also be deployed to HCO patients, to provide a secure online method to access individual health care records. Patients will now be authenticated and granted authorization privileges into the private records from any "Authorization Gateway" enabled terminal.

eMarketplaces and ASPs

ASPs and eMarketplaces are increasingly incorporating security- related authentication and access control services as native components of their architecture. Organizations are also beginning to demand access and authorization requirements into their ASP and eMarketplace products and services. Sac's early efforts have focused on developing these identity and authentication services to layer directly into an eMarketplace or ASPs current service offerings.
Some of the practical everyday applications could be:

- Customized credit card accounts where users are limited on where and what types of goods can be purchased based on purchasing authority
- Student purchase cards
- Government purchase cards
- Employee purchase cards that limit only approved purchases based on company guidelines

Features & Benefits

- SOAP/XML interface for developers
- Web-interface for configuration
- The web-interface used for requesting certificates
- Policies can be modified on-the-fly
- Can be installed on any Windows/Linux/Unix server
- A hardware-based encryption device can be used to facilitate file encryption, private key protection and SSL acceleration.

Product Code	Product Name	SIN	Retail Price	GSA Price
TAG-MD5000	Transaction Authorization Gateway Medium Business	132-3	$1,650,000	$1,500,000
TAG-LG-10000	Transaction Authorization Gateway Large Business	132-3	$2,750,000	$2,500,000
TAG-ENT	Transaction Authorization Gateway Enterprise	132-3	$5,280,000	$4,800,000
TAG-MAINT	Transaction Authorization Gateway Maintenance Fees (20% of annual licensing fees)	132-34	25%	20%
TAG-INSTALL	Transaction Authorization Gateway Installation Fees ($2,000 per day – 5 day minimum)	132-3	$2,200	$2,000
TAG-TRAIN	Transaction Authorization Gateway Training Fees ($2500 per day for up to 15 students – 4 days recommended)	132-50	$2,700	$2,500

SAC Enterprise Replicator

Today many organizations are faced with an impending problem of managing policies, literature, engineering documents, compliance regulations, critical records etc. These organizations in many cases are not only challenged with version control and change management control but also the associated risks assigned to not having a robust next generation document management solution in place. Attempting to organize policies across disparate business units can become a nightmare in dispersed or virtual organizations.

In complex organizations, training documents, HR and security policies must be accurate and up to date all the time. Just as importantly, compliance documents that cover usage guidelines that protect companies from exposure to outside threats based on which websites should not be visited in conjunction to varying viral threats can make the need for data, document and information consistency imperative.

Imagine creating an information management system that managed information at the user level, which also ensured that authors and originators of source documents could always maintain version control, and provide the organization with the most up to date information no matter when, or where the user was located as long as they were able to connect to the enterprise network. If this system could not only ensure document authenticity, but also manage change control as well as enforce Digital Rights Management in real-time for every document stored within the system.

Server replication

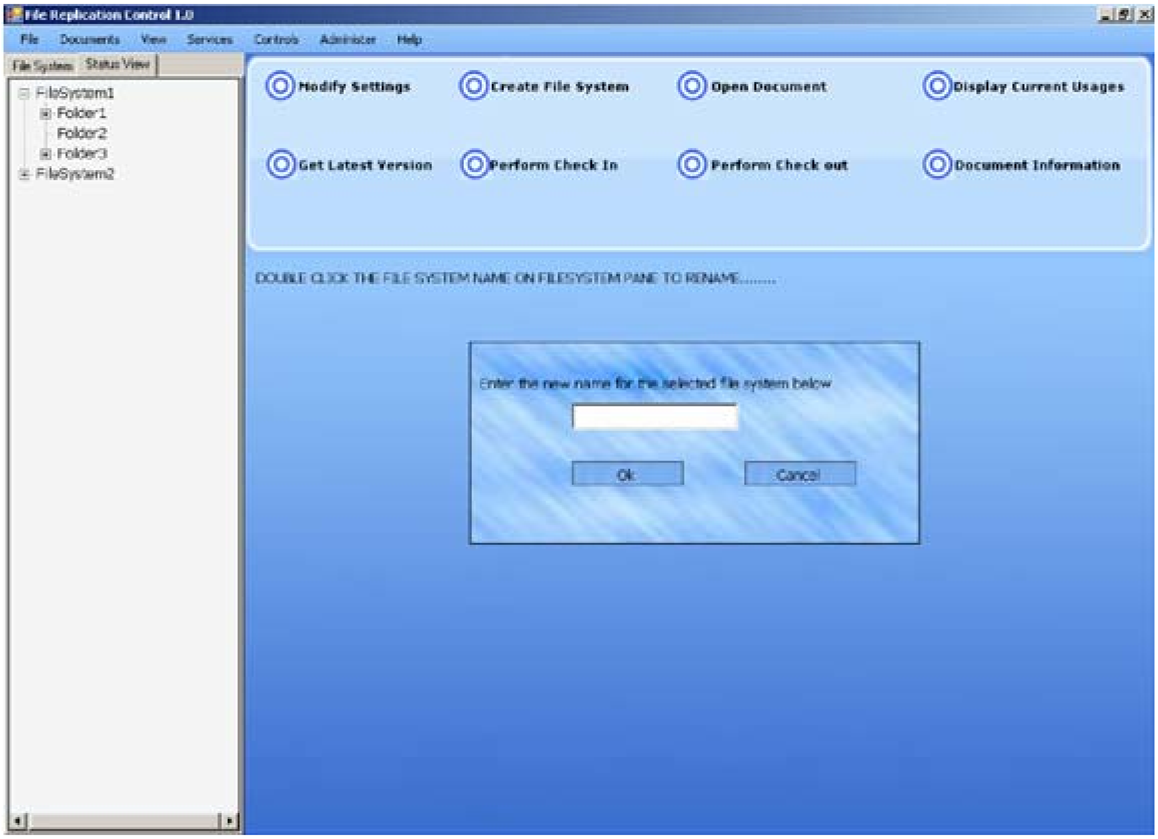
Continuous 2-Way Real-time Mirroring of application data that resides on two active production servers located on the same network.

In this configuration, two active servers are operating on the same subnet. First, SAC agents are installed on any device. Next, a Replication profile is configured on Server A to replicate its data directory to Server B's identical data directory. Likewise, a Replication configuration is set up on Server B to replicate its data directory back to Server A's data directory. Thus each time a file is updated, on either server, it is immediately replicated to the other server maintaining data synchronization, usually within seconds. This is especially useful in those cases where the servers are sharing the user access load on the network. Another major benefit is the redundancy of the servers. If one server goes down the remaining server can service the user base until the other server is restored to operation.

Data Replication

Now enter the desktop age where individuals check out documents and make changes to those documents continuously. By enabling change management technology with the ability to replicate at the desktop level instead of having just server to server redundancy we've created actual data to data redundancy across the enterprise. Data replication gives users the flexibility to make changes anywhere in the network while having those changes along with full digital rights management compliance enforcement in place to manage what data belongs on users desktops and company servers and what data or version does not(this sentence is too long we need to break it up so it flows well). Where traditional replication software fails to enforce compliance across the enterprise due to limitations of server to server mirroring, Security Associates has gone two steps further giving you replication at the data level, not only with documents, but any type of file as well.

The ability to rename and republish entire file systems globally



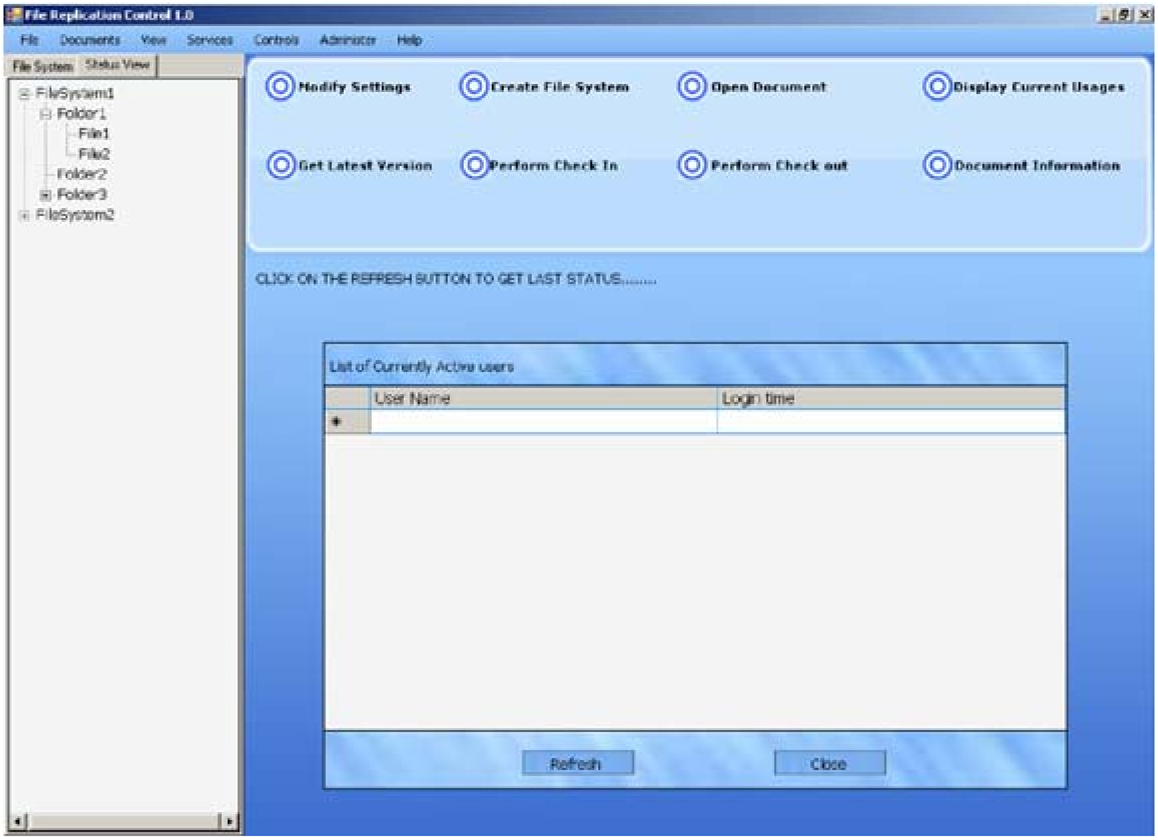
DOUBLE CLICK THE FILE SYSTEM NAME ON FILESYSTEM PANE TO RENAME........

Enter the new name for the selected file system below

Whether you're checking software in and out, or making changes to policies and procedures, you can ensure your enterprise is up to date with the latest policies and procedures in real time with Security Associates Enterprise Explorer. Expanding on this we have the ability to take a peek at any system connected on the network as long as they have an IP and validate their data, systems, e-mails, and software are in compliance in real-time.

File Replication Control system is a high performance document management and version control solution used to organize and protect an organizations file based information assets. It provides the flexibility of maintaining disparate files across large numbers of users in a secure, controlled manner while ensuring data integrity, availability, and policy based access control as well as full auditing and logging.

View Status of Users Currently Working on Documents across the entire Enterprise



CLICK ON THE REFRESH BUTTON TO GET LAST STATUS........

List of Currently Active users

	User Name	Login time
*		

The File Replication Control solution allows users to make changes from a central location that can affect all associated documents across the enterprise. With the ability to provide change and version control in conjunction with digital signing, this product provides the most robust document management features in the market today.

Product Code	Product Name	SIN	Retail Price	GSA Price
REPSB100	Replicator Small Business Level 1 (1 to 100 users)	132-3	$11,000 (per server)	$10,000 (per server)
REPSB500	Replicator Small Business Level 2 (101 to 500 users)	132-3	$55,000 (per server)	$50,000 (per server)
REPMD1000	Replicator Medium Business Level 1 (501 to 1,000 users)	132-3	$165,000 (per server)	$150,000 (per server)
REPMD5000	Replicator Medium Business Level 2 (1,001 to 5,000 users)	132-3	$330,000 (per server)	$300,000 (per server)
REPLG10000	Replicator Large Business (5,001 to 10,000 users)	132-3	$550,000 (per enclave)	$500,000 (per enclave)
REPSL	Replicator Site License (10,001 to 25,000 users)	132-3	$1,650,000	$1,500,000
Pricing for 25,0001 users and above is cumulative of above products (e.g., 25,0001 users would require REPSL and REPSB100; 25,110 users would require REPSL and REPSB500, etc.)				

SAC Enterprise Explorer – Centralized Configuration Security Document Data Architecture:

Centralized configuration and security:

SAC has developed three tiered application for a centralized security document management. That has the ability to perform contextual based searches. The enterprise solution not only works for searching files and documents, but emails as well.

Since the product is an enterprise search engine any and all keywords that exist across the entire network can be searched so determining if out of date content exists can be accomplished at the enterprise level. The key strength of a solution such as this is outdated, unauthorized, or privileged information can be located down to the user desktop now without having to guess what exists in the enterprise any longer.

With a dedicated search server designed to index and perform complex context based searches the amount of time to locate documents is reduced significantly allowing system resources to remain freed up for other critical tasks.

The Document Server:

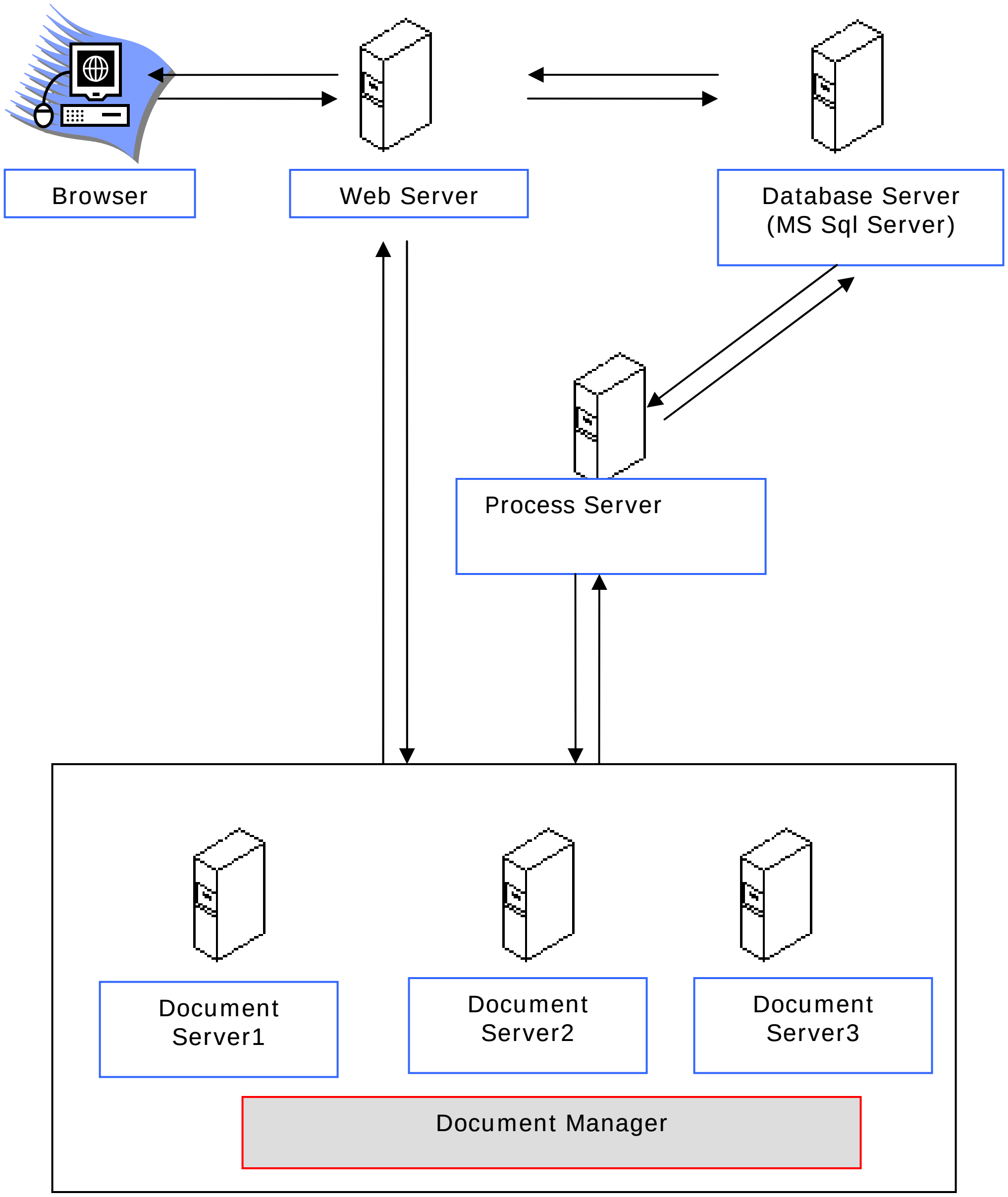
The Document Server maintains all document servers, groups and users. It has a service and user interface for centralized configuration and views of all objects .

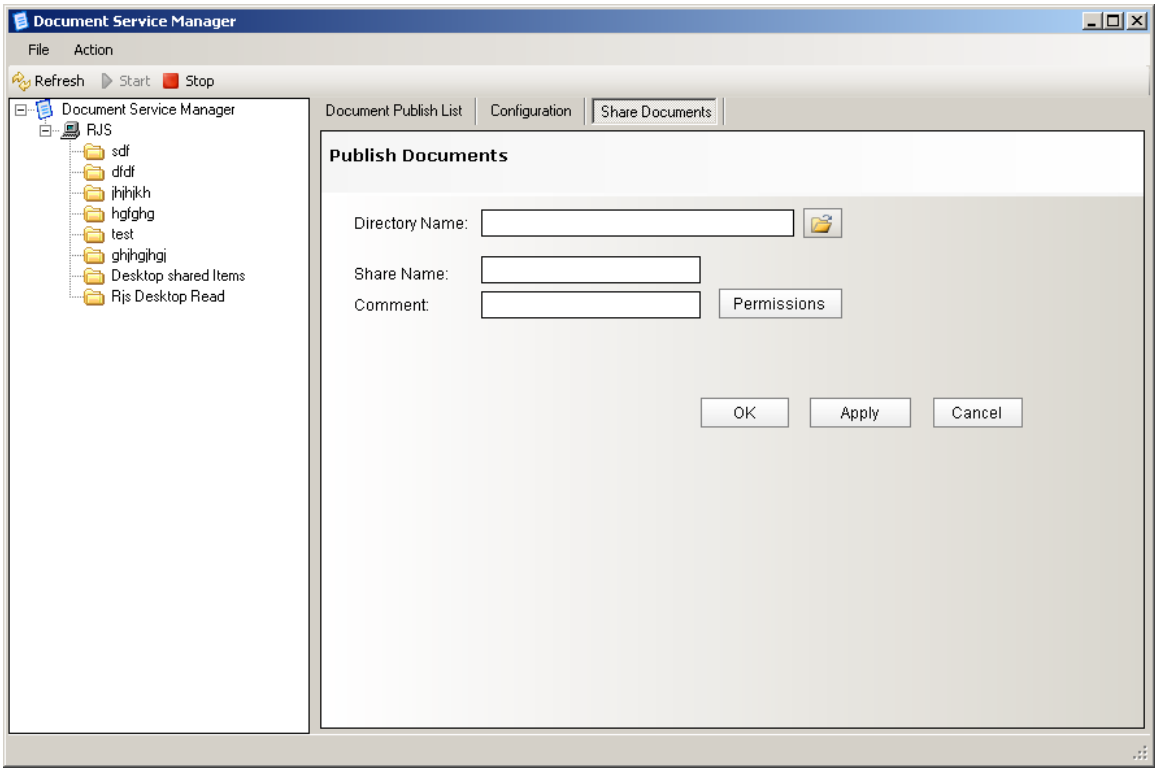
The Document Manager:

Using this application user can publish documents across the network. Here a user configures the Document Manager. Users can also make changes to master documents to be replicated across the enterprise.

Web Client:

This Browser based application and the purpose of this application is to access server resources from the client browser.


Browser
Web Server
Database Server
(MS Sql Server)
Process Server
Document
Server1
Document
Server2
Document
Server3
Document Manager


Document Service Manager
File
Action
Refresh
Start
Stop
Document Service Manager
RJS
sdf
dfdf
jhjhjkh
hgfghg
test
ghjhgjhgj
Desktop shared Items
Rjs Desktop Read
Document Publish List
Configuration
Share Documents
Publish Documents
Directory Name:
Share Name:
Comment:
Permissions
OK
Apply
Cancel

Product Code	Product Name	SIN	Retail Price	GSA Price
EESB100	Enterprise Explorer Small Business Level 1 (1 to 100 users)	132-3	$7,700	$7,000
EESB500	Enterprise Explorer Small Business Level 2 (101 to 500 users)	132-3	$44,000	$40,000
EEMD1000	Enterprise Explorer Medium Business Level 1 (501 to 1,000 users)	132-3	$137,500	$125,000
EEMD5000	Enterprise Explorer Medium Business Level 2 (1,001 to 5,000 users)	132-3	$275,000	$250,000
EELG10000	Enterprise Explorer Large Business (5,001 to 10,000 users)	132-3	$495,000	$450,000
EESL	Enterprise Explorer Site License (10,001 to 25,000 users)	132-3	$1,320,000	$1,200,000
Pricing for 25,0001 users and above is cumulative of above products (e.g., 25,0001 users would require EESL and EESB100; 25,110 users would require EESL and EESB500, etc.)				

ThreatGuard Network Security Appliance

Continuous Vulnerability Awareness and Asset Management

What is ThreatGuard?

ThreatGuard is a continuous vulnerability and asset management system. The ThreatGuard appliance can be placed internal or external to an organization’s network, and continuously scans the network for new security risks including spyware and application vulnerabilities. It gathers hardware and software information about each discovered host for use in asset tracking and change management. ThreatGuard includes functions vital to a comprehensive security scan, such as continuous network mapping and host detection, comprehensive port scanning, operating system detection, and vulnerability scanning. When new machines appear on the network, they are automatically detected and scanned for vulnerabilities that could allow unauthorized intruders access to private information. The ThreatGuard appliance automatically downloads new vulnerability updates and software changes from ThreatGuard's central database on a daily basis without requiring administrative intervention. ThreatGuards can be stand-alone or organized in a hierarchy, providing centralized management and security posture reporting. Managers and technicians can view security posture through a variety of reports and are also able to prioritize and assign “fix-it” tasks to employees. These assignments are tracked using the integrated vulnerability lifecycle management tools.

What problems does ThreatGuard address?

ThreatGuard addresses some fundamental but endemic problems faced by all organizations with information technology infrastructure.

- How many and what type of devices are attached to the network?
- What software and services are running on these devices?
- What security vulnerabilities exist on each device?
- How do I manage the mitigation of these vulnerabilities?
- What is the security posture of my entire network?

How are all of the above items tracked over time?

Simply knowing the number and type of devices connected to networks is an ongoing challenge for most organizations. The ThreatGuard appliance uses a variety of methods to detect devices that are attached to the network. Once detected, each device is analyzed to determine its hardware and software configuration. This information is used by the system to conduct targeted asset and vulnerability evaluation.

A vulnerability represents an error or an oversight on a computer system that allows a perpetrator to perform actions with the computer that the owner of the resource did not intend. The actions these perpetrators perform include tying up the machine so that it can no longer reliably perform its intended function, known as a DoS (Denial of Service) attack, using it to distribute illegal software (Warez), using it as a launching point for other attacks, web site defacement, or stealing valuable information as exemplified by the credit card theft cases that frequently make the headlines.

The methods used also vary widely. A DoS attack, for example, might take advantage of the *chargen* and *echo* services, available after the default installation of many operation systems, to flood the local network and tie up the processors on the machines involved. An easy example that will give a remote attack immediate root-level access to any unpatched Sun Solaris server (Solaris versions 2.3, 2.4, 2.5.1, 2.6, and 7) is the RPC *sadmind* service, which, again, is installed and active by default (or, in the case of 2.3 and 2.4, as part of the Solstice Adminsuite). As a further example, misusing a machine often requires no level of access at all: CGI (Common Gateway Interface), a typical method for extending the usability of a website, and SQL (Structured Query Language) attacks can quite often be performed just by altering the URL that a web browser sends to the web site.

Since there are a large number of tools that automate the process of taking advantage of these weaknesses, the technical complexity of an exploit is rarely a barrier for even the most unskilled of attackers. And while there are pros and cons to the existence of these tools, the inescapable fact is that they do exist.

A vulnerability assessment is a reconnaissance of devices attached to the network to discover what possible avenues of attack exist. It generally consists of a series of tests that probe for specific known weaknesses. The tests used by the ThreatGuard represent a combination of known security holes, rule sets based on many years of combined administrative experience, and best practices. For example, *daytime* is a simple service typically active by default that currently has no known vulnerabilities. However, it's very rare that it is needed, so disabling it means you will not be susceptible if a vulnerability is found. The results of a vulnerability assessment include a list of vulnerabilities on each host and a description, mitigation steps, and the relative severity for each vulnerability.

The vast majority of current products treat vulnerability assessments as one-time tasks. These "scans" can easily take hours or days to complete and are outdated as soon as a new machine is added to the network, a system is reloaded, or a new vulnerability is discovered that applies to a version of software running on the network. The automatic update feature combined with its continuous scanning capabilities and e-mail notification allow ThreatGuard to provide near real-time vulnerability status information.

Why is vulnerability management important?

According to CERT/CC (Computer Emergency Response Team/Coordination Center, a center of computer security expertise sponsored by Carnegie Mellon University), 99% of all reported intrusions “result through exploitation of known vulnerabilities or configuration errors for which countermeasures were available.”

The process of keeping track of all of these vulnerabilities, their impact, knowing how to test for them, and what fixes to apply, is a very time-consuming task, even on a fairly homogeneous network. In the best of times, very few IT (Information Technology) shops have the additional man hours necessary to keep track of all of the historical and current vulnerabilities, let alone have an easy way to validate that all fixes have been applied to all devices on the network. In times of poor economic performance, IT, usually viewed as a cost center, is one of the first places to experience budget cuts.

ThreatGuard vulnerability discovery process.

The assessment is broken up into several discreet steps:

- Discovery. Once a range of addresses to assess has been entered into the system, it first uses a fast, low-bandwidth test to determine which of those addresses have devices currently running on them. The system will re-test on a fairly frequent basis, thus learning when machines are added to or removed from the network.
- Service Mapping/Detection. For every active address on the network, every single service port is tested to determine whether or not a service is running at that port --that's 65535 TCP and 65535 UDP ports. In many cases, it is also possible to positively determine which service is running on that port, thus greatly reducing the number of security tests that need to be performed across the wire and therefore reducing the impact on the target machine and the network.
- Targeted Vulnerability Tests. Based on the results from above, a list of tests that apply to each open port is assembled and run. Additionally, ThreatGuard can authenticate into machines to perform targeted on-box security evaluations of services and applications. The results of these tests are saved in a relational database that is embedded in the ThreatGuard, and can be used to further target any remaining tests.
- Knowledge Mining. After a test run, a second class of test is performed using the full set of results --both positive and negative --as well as, potentially, results from other ThreatGuards that are reporting on other network segments.

ThreatGuard capabilities.

- Ease Of Use. In the simplest case, use of ThreatGuard can reduced to the following three steps:
  1) Configure the IP address of the ThreatGuard.
  2) Install the client application on an administrative workstation.
  3) Type in the range if IP addresses to be scanned and make that range active.
- From there, the box will perform a full analysis on all machines within that list of addresses, keep itself updated, keep track of all changes to machines in that list as they occur, and make a wide variety of reports available at any time. More advanced users can take advantage of many of its other features as well. Continuous. Rather than perform its tasks a single time and halt, the ThreatGuard gently re-checks the range of machines it has been assigned throughout the day, keeping tracks of changes, new machines, new vulnerabilities and patched vulnerabilities, and even tracking machines if they move from one network to another. This means that a technician does not need to run a new scan and wait hours or days for the results, but can simply log on to the ThreatGuard to get current vulnerability status information. Other benefits include the immediate re-testing after a technician marks a vulnerability as fixed, and immediate testing for new vulnerabilities after the box updates itself with new vulnerability detection information. ThreatGuard is designed to have minimal impact on the network. Using the default values, the ThreatGuard rarely reaches 5% of a 10 MBps network. The aggressiveness of the scanning engine can be changed by the ThreatGuard user.

- Hierarchical. More than one ThreatGuard can be tied together with a designated “Master” acting as a central controller over the others. In this way, when it is necessary for reasons of network topology, geographic distribution, or even politics, to use multiple ThreatGuards in evaluating an entire organization, individual tasks can still be controlled from a single location, and summary data replicated back to that controlling node. This makes it possible to get a quantifiable view of the security posture of an entire organization into a single chart or report, and also allows for knowledge mining across the entire organization.
- Automated Updating. By default, the ThreatGuard checks for updates on a regular basis via the Internet. Normally these updates are new vulnerability tests, but they can also include changes to the scanner, new reports, or even changes to the host operating system. In circumstances where the Internet is not accessible from where the ThreatGuard is used, updates can be made via a CD image. When new vulnerability updates are received, the ThreatGuard will immediately check these against all hosts that might be susceptible. And because the ThreatGuard is a continuous scanner, it is only necessary to re-scan for the new vulnerabilities rather than wait for a complete re-scan, and thus the current security status of the target network is known in as quickly as a few minutes.
- Workflow Management. Included with the ThreatGuard is a system for assigning and tracking vulnerability mitigation efforts. This allows for automatic or manual assignments of vulnerabilities to specific technicians, email notification as new vulnerabilities are found, a record of what is fixed and by whom, and a record of vulnerabilities chosen to be ignored and why. This workflow system also includes an escalation capability that automatically reassigns vulnerabilities if they are not fixed by their assigned due dates.
- Rich Reporting. The reporting system available in the ThreatGuard system comes with a series of reports targeted from an executive-level overview down to the technician level, with all the details necessary to understand the impact of any vulnerability and make the necessary corrections. ThreatGuard provides additional reports that show security posture trends of hosts and networks over time. Reports can be exported to PDF, HTML, CSV, XLS, and XML formats.
- Relational Database. Every ThreatGuard comes with an embedded relational database, where all preferences, settings, asset, and assessment results are stored. The key benefits are that adding new tests becomes much easier, details from specific security tests can be used by more than one test, relieving the need to constantly re-query the target machine across the network, easy support of a very dynamic and extensible reporting system including trend analysis, and knowledge mining. The database also allows for historical data to be saved. Along with trend analysis reports, this also makes changes obvious, such as when a server is rebuilt but some of the patches are forgotten. Further, this database is resident on the local network so information gathered never leaves the hands of the ThreatGuard owner.
- Secure Communications. All communications, both from the client application and the ThreatGuard, and when one ThreatGuard transfers data to another, is done via a proprietary secure, encrypted communication mechanism.
- Extensible. The system has been designed to easily allow other classes of functionality to be added to the ThreatGuard. For example, an enhanced asset management tracking system is currently under development that will extend the capabilities of current ThreatGuard systems. ThreatGuard also offers the General Purpose Link System (GPLS) that allows third-party integration via an embedded SOAP server.

Network-based scanning limitations.

- "Zero-Day Hacks"

  What it is: An exploit that has never been used or published before. Most new exploits take advantage of a vulnerability that is already known, but on occasion a new exploit is developed against a vulnerability that was never known publicly. For this type of exploit, which is estimated to comprise less than 1% of all security breaches, there will be no vulnerability test until after the fact.

  How ThreatGuard handles this limitation: There will always be a development and testing time delay between the discovery of a new vulnerability and its availability to the end-user. By automatically checking for and applying new vulnerability tests as soon as they are available, the ThreatGuard greatly reduces the time between the discovery of a new vulnerability and the knowledge of whether or not a machine is susceptible to it.

- Remote Networks

  What it is: A network of computers separated by a networking device, such as a router. Such a device almost always limits to some degree the network traffic that flows across it, so that the full scope of networking options available locally are not necessarily available on the remote side.

  How ThreatGuard handles this limitation: The vast majority of the tests performed by the ThreatGuard use TCP/IP packets which should flow unhindered across network devices. There are some instances, such as if an ACL (Access Control List) has been applied to deny certain ICMP messages, where portions of the scanner may not produce results that accurately reflect the true conditions on the remote network. Placing a second ThreatGuard on the remote network and pooling the data will relieve this problem.

- Bandwidth

  What it is: Testing for vulnerabilities on hosts generates network traffic. On very slow networks or saturated links, the amount of traffic generated may be enough to cause degradations in network performance.

  How ThreatGuard handles this limitation: The ThreatGuard has been developed to produce as little network traffic as possible. It does this through a variety of methods, such as pruning out all tests that don't apply to a specific target, and using the embedded database to store results from one test that can be used for other tests. The ThreatGuard also contains a full set of behavioral settings that can further reduce (or increase) network traffic. Using the scan controls to reduce the amount of bandwidth utilized by the ThreatGuard will have the side effect of increasing the amount of time to perform the evaluation. In cases where local networking is fine but connecting links are saturated, using more than one ThreatGuard can solve the problem.

- Remote testing vice on-box

  What it is: Testing remotely across the network is not always precise, and is impractical for other types of security information. For example, it is possible to determine the password lockout policy by using a login service such as telnet and noting when it stops responding for that user. Unfortunately, this method could also easily lock out a legitimate user account and require administrative action to enable it again.

  How ThreatGuard handles this limitation: Using supplied credentials, ThreatGuard can authenticate over the network into Microsoft Windows, Unix, and Unix-like operating systems to perform on-box asset and security analysis. This allows the system to gather very precise information about hardware configuration, installed applications, services, and accounts.

ThreatGuard Compliance & Vulnerability Management System

Automated Compliance and Vulnerability Management

What is ThreatGuard CVMS?

ThreatGuard CVMS is an automated compliance and vulnerability management system. It addresses both major components of technical security: compliance and vulnerabilities while providing automated remediation of findings. ThreatGuard CVMS performs assessments to ensure devices comply with standards such as FISMA and DISA STIGS. It also evaluates each system to detect vulnerabilities and assess the status of security patches. Compliance testing is done using the National Institute of Standards and Technology (NIST) automated XCCDF checklists (as part of their Security Content Automation Program or SCAP) with the user choosing the appropriate security level, for example FISMA Enterprise Moderate. All compliance and vulnerability tests are done using the Open Vulnerability Assessment Language (OVAL). All scoring of devices during the vulnerability management are made using the Common Vulnerability Scoring System (CVSS).

The system provides documented reporting of configurations pre and post remediation and provides automated remediation of non-compliant items. ThreatGuard CVMS includes a remediation undo feature that resets the computer to pre-remediation state. For new vulnerabilities discovered, the system provides manual instructions for remediation and output in OVAL and other formats for automated remediation if the client so chooses. Records of vulnerabilities found and fixed are kept for use by inspectors or auditors. ThreatGuard CVMS includes functions vital to a comprehensive security scan, such as network mapping and host detection, comprehensive port scanning, operating system detection, and vulnerability scanning. When new machines appear on the network, they are automatically detected and scanned for vulnerabilities that could allow unauthorized intruders access to private information. Workflow management is available for those choosing manual remediation. ThreatGuard CVMS can operate using agents, agentlessly, as a Service Oriented Architecture (SOA) or any combination of the three.

What problems does ThreatGuard CVMS address?

ThreatGuard addresses some fundamental but endemic problems faced by all organizations with information technology infrastructure.

- How does one ensure correct configuration for compliance and prove it?
- How do I identify and document exceptions to compliance policies?
- How many and what type of devices are attached to the network?
- What software and services are running on these devices?
- What security vulnerabilities exist on each device?
- How do I manage the mitigation of these vulnerabilities?
- What is the security posture of my entire network?

Why does my organization need ThreatGuard CVMS?

In the past, compliance has been a manpower intensive affair. For example, there are 408 technical rules one must comply with for a FIMA Enterprise High security posture on Windows XP. To perform checks and remediation on 408 items would take many hours to perform manually. With NIST’s development of automating checklists, ThreatGuard CVMS can perform the assessment for those 408 items in less than 10 seconds. After reviewing the references to see why items failed, you can use ThreatGuard CVMS to perform automated remediation. If you don’t like the results, hit the undo button to return to the previous configuration. You can do this manually machine by machine or across the network. The frequency of compliance checks is up to the user.

Simply knowing the number and type of devices connected to networks is an ongoing challenge for most organizations. The ThreatGuard CVMS uses a variety of methods to detect devices that are attached to the network. Once detected, each device is analyzed to determine its hardware and software configuration. This information is used by the system to conduct targeted asset and vulnerability evaluation.

Why is vulnerability management important?

According to CERT/CC (Computer Emergency Response Team/Coordination Center, a center of computer security expertise sponsored by Carnegie Mellon University), 99% of all reported intrusions “result through exploitation of known vulnerabilities or configuration errors for which countermeasures were available.”

A vulnerability represents an error or an oversight on a computer system that allows a perpetrator to perform actions with the computer that the owner of the resource did not intend. The actions these perpetrators perform include tying up the machine so that it can no longer reliably perform its intended function, known as a DoS (Denial of Service) attack, using it to distribute illegal software (Warez), using it as a launching point for other attacks, web site defacement, or stealing valuable information as exemplified by the credit card theft cases that frequently make the headlines.

The process of keeping track of all of these vulnerabilities, their impact, knowing how to test for them, and what fixes to apply is a very time-consuming task, even on a fairly homogeneous network. In the best of times, very few IT (Information Technology) shops have the additional man hours necessary to keep track of all of the historical and current vulnerabilities, let alone have an easy way to validate that all fixes have been applied to all devices on the network. In times of poor economic performance, IT, usually viewed as a cost center, is one of the first places to experience budget cuts.

ThreatGuard vulnerability discovery process.

The assessment is broken up into several discreet steps:

- Discovery. Once a range of addresses to assess has been entered into the system, it first uses a fast, low-bandwidth test to determine which of those addresses have devices currently running on them. The system will re-test on a fairly frequent basis, thus learning when machines are added to or removed from the network.
- Service Mapping/Detection. For every active address on the network, every single service port is tested to determine whether or not a service is running at that port --that's 65535 TCP and 65535 UDP ports. In many cases, it is also possible to positively determine which service is running on that port, thus greatly reducing the number of security tests that need to be performed across the wire and therefore reducing the impact on the target machine and the network.
- Targeted Vulnerability Tests. Based on the results from above, a list of tests that apply to each open

port is assembled and run. Additionally, ThreatGuard can authenticate into machines or remotely activate agents to perform targeted on-box security evaluations of the operating system, services and applications. This can be controlled centrally by third-party systems using SOA.

- Knowledge Mining. After a test run, a second class of test is performed using the full set of results --both positive and negative --as well as, potentially, results from other ThreatGuard CVSS's that are reporting on other network segments.

ThreatGuard features and capabilities.

- Complete compliance assessment using industry standard XCCDF and OVAL content
- Remediation. ThreatGuard CVMS can automatically remediate non-compliant configuration items to their compliant state.
- Multi-level Undo. If remediation of particular items is found to cause problems, remediation for those items can be rolled-back to the original state. Additionally, all remediation changes on a computer can be automatically rolled-back to their original configuration.
- Policy Exception/Waivers. If certain policy requirements are found to cause operational problems on a system, ThreatGuard CVMS provides a mechanism to override those settings and generate a detailed waiver request.
- Automatic Update. All ThreatGuard CVMS components contain automatic update capabilities ensuring applications and content are updated and current on a daily basis.
- Flexibility. ThreatGuard CVMS comes in a variety of configurations and components to best suite unique organizational needs. From agents to appliances, ThreatGuard CVMS is the most flexible and customizable solution on the market.
- Ease Of Use. All ThreatGuard components are designed to be easy to install and operate. For example, in the agentless appliance mode, use of ThreatGuard CVMS can reduced to the following three steps:
    1. Configure the IP address of the ThreatGuard CVMS.
    2. Install the client application on an administrative workstation.
    3. Type in the range if IP addresses to be scanned and make that range active.
- Hierarchical. More than one ThreatGuard CVMS can be tied together with a designated "Master" acting as a central controller over the others. In this way, when it is necessary for reasons of network topology, geographic distribution, or even politics, to use multiple ThreatGuard CVMSs in evaluating an entire organization, individual tasks can still be controlled from a single location, and summary data replicated back to that controlling node.
- Workflow Management. Included with the ThreatGuard CVMS is a system for assigning and tracking vulnerability mitigation efforts.

- Rich Reporting. The reporting system available in the ThreatGuard CVMS system comes with a series of reports targeted from an executive-level overview down to the technician level, with all the details necessary to understand the impact of any vulnerability and make the necessary corrections. ThreatGuard provides additional reports that show security posture trends of hosts and networks over time. Reports can be exported to PDF, HTML, CSV, XLS, and XML formats.
- Extensible. The system has been designed to easily allow other classes of functionality to be added to the ThreatGuard CVMS.
- Interoperability. ThreatGuard CVMS is designed to integrate seamlessly with other systems using industry standards including exporting of OVAL results files and system control via SOA.

ThreatGuard CVMS Traveler

ThreatGuard CVMS Traveler is a virtual security appliance that is placed internal or external to an organization's network. ThreatGuard CVMS Traveler is designed to support a variety of network security functions, including network discovery, assessing configuration/compliance, determining vulnerabilities of applications and port scanning.

The ThreatGuard CMVS Traveler contains all of the capabilities of a traditional ThreatGuard CMVS system, but is designed for mobile use. In Travel configuration, the ThreatGuard CMVS provides limited re-scan capabilities of any given network.

ThreatGuard's team of security engineers constantly monitors government, vendor, and security resources to identify new compliance checklists and new vulnerabilities. Using our rapid update process, we quickly create tools to automatically use the compliance XCCDF checklists and detect these new vulnerabilities.

Key features of ThreatGuard CVMS Traveler:

- Uses industry-standard XCCDF and OVAL compliance, vulnerability, and patch assessment content
- Compliance monitoring for the security level selected, such as FISMA Enterprise Moderate
- Automated remediation of non-compliant items
- Multi-level remediation undo feature
- Compliance exception and waiver creation capability
- Anonymous host discovery and categorization system
- Comprehensive port scanner and service enumeration
- Continuous or on-demand compliance, vulnerability, and patch assessment
- Automatic bandwidth monitoring & throttling (Prevents flooding the network during evaluation)
- Data export in a variety of common formats including OVAL results format
- Auto-update system to keep application and assessment content current

ThreatGuard Secutor Magnus

What is ThreatGuard Secutor Magnus?

Secutor Magnus is the first product designed specifically to meet the Common Security Configurations requirements set forth by the Federal Government's Office of Management and Budget (OMB). Built for the "Information Security Automation Program" (ISAP) as established by the National Institute of Standards and Technology (NIST), Magnus fully supports a wide-scale action plan to quickly and continually show that an organization has compliance under control. The entire Secutor line of automated content tools provides standardized assessments, content-driven remediation, and complete mappings to driving requirements with options to easily document deviations from those requirements. With over 800 evaluators from government, military, commercial, and academic locations, Secutor provides operational confidence to network administrators, system integrators, and IT service providers. NIST has ushered in a new era of standards-based compliance assessment. Secutor Magnus meets those standards to the fullest, and extends them to be a complete compliance solution.

Key Features:

Test NIST configurations to identify adverse effects on system functionality.

- Desktop module places a system in 100% compliance in under 60 seconds.
- Selective undo/redo/restore supports quick adjustments to test effects.
- System profiler exports deviations for operational assessments and remediation.

Automated enforcement

- Magnus scheduler periodically assesses compliance across the network.
- Notifications alert specified personnel when systems fall out of compliance.
- Optional setting to reapply remediation on detection of altered systems.

Restrict administration to authorized professionals

- Magnus requires proper credentials to view and apply settings.
- Executive-level views permit read-only access to compliance status.

Ensure new acquisitions use standard configurations

- Desktop module can enforce standards prior to deployment of new systems.
- Operational profiles apply authorized deviations during lockdown procedures.

Patches

- Automatically determines if computers have all required security patches.
- Performs vulnerability assessment of operating system and major applications.

Provide documentation of deviations with rationale

- System profiler enables simple, yet full-featured deviation system, including accountability, documentation, expiration, traceability to requirements, and recognition during assessments and remediation.

Architecture and supported platforms

- Windows XP, Window Vista, Windows Server 2003 – more platforms will be added as NIST releases content including Solaris and Red Hat Linux.
- Requires Microsoft .NET 2.0 or greater (included).

ThreatGuard Secutor Magnus features and capabilities:

- Complete compliance assessment using industry standard XCCDF and OVAL content
- Remediation. ThreatGuard Secutor Magnus can automatically remediate non-compliant configuration items to their compliant state.
- Multi-level Undo. If remediation of particular items is found to cause problems, remediation for those items can be rolled-back to the original state. Additionally, all remediation changes on a computer can be automatically rolled-back to their original configuration.
- Policy Exception/Waivers. If certain policy requirements are found to cause operational problems on a system, ThreatGuard Secutor Magnus provides a mechanism to override those settings and generate a detailed waiver request.
- Automatic Update. All ThreatGuard Secutor Magnus components contain automatic update capabilities ensuring applications and content are updated and current on a daily basis.
- Flexibility. ThreatGuard Secutor Magnus comes in a variety of configurations and components to best suite unique organizational needs. From agents to appliances, ThreatGuard Secutor Magnus is the most flexible and customizable solution on the market.

ThreatGuard Secutor Prime Standard

Overview

Secutor Prime is the first product to perform automated compliance evaluation and remediation using the U.S. Government's new automated content standard. Developed by the National Institute of Standards and Technology (NIST) for the Federal Government, this standards-based content represents the definitive guidance for FISMA compliance assessment and includes automated content for DISA STIGS Gold and Platinum and NSA guides. By integrating various government sponsored initiatives, including the eXtensible Configuration Checklist Description Format (XCCDF) and the Open Vulnerability and Assessment Language (OVAL), NIST has ushered in a new era of standards-based compliance assessment and remediation. Secutor Prime is the first product to turn the vision of automated security compliance into reality.

Key Features:

Use of NIST Security Content Automation Files

- Direct consumption of NIST-developed XCCDF and OVAL definition content.
- User can specify the name and location of the XML configuration files to use.
- Provides mapping of security checks to governing requirements.
- Provides runtime notes – allowing auditors and security engineers to verify and validate assessment decisions.

Security Patch Checks & Vulnerability Assessment

- Automatically determines if computers have all required security patches.
- Performs vulnerability assessment of operating system and major applications.
- Automated update system keeps application and assessment content current.

Configuration and Security Remediation & Undo

- If discrepancies are discovered, Secutor Prime can automatically modify the configuration and security settings to bring systems into compliance.
- Secutor Prime can fix all problems or just those selected by the user.
- Reassessment occurs to validate remediation and ensure compliance.
- Perform remediation undo of individual rules or full system restore.

Standards-Based Assessment System

- Incorporates optimized XCCDF document parsing engine.
- Supports OVAL version 5.x as a definitions evaluator.
- Includes the first assessment engine to pass OVAL 5.0 certification testing.
- Support for Common Vulnerabilities and Exposures (CVE), Common Configuration Enumeration (CCE) and Common Vulnerability Scoring System (CVSS) when content becomes available.

Security Reporting & Data Export

- Includes HTML-based reports suitable for printing and drill-down.
- Secutor Prime report shows summary and detailed benchmark scoring.

- Exports CSV, OVAL thin and full results files, compressed or uncompressed.

Architecture & Supported Platforms

- Windows XP, Vista, 2003 Server, and 2000 - more as NIST releases content.
- Requires Java Run-time Environment 1.4x or greater (included).

ThreatGuard Secutor Prime Professional

Overview

Secutor Prime Professional pushes Secutor Prime to a new level. Professional includes all the powerful features of Prime and adds official OMB FDCC Deviation Report generation and agentless assessments of remote targets. The Secutor Prime product line was the first to support automated compliance evaluation, deviation management, and remediation using the U.S. Government's new automated content standard. Developed by the National Institute of Standards and Technology (NIST) for the Federal Government, this standards-based content represents the definitive guidance for Federal Desktop Core Configuration (FDCC) and FISMA compliance assessment.

Key Features:

Generate OMB-Required FDC Deviations Report

- Identify and define deviations to the FDCC and generate the standard report for submission to OMB.
- Produces required XML file and a human-readable HMTL version.

Manage Compliance from a Single Location

- Perform Secutor Prime compliance tasks on remote computers agentlessly.
- Leverages the CPE standard to determine applicable benchmarks for targets.
- Track deviations and generates assessment reports from a single desktop.

Use of NIST Security Content Automation Files

- Direct consumption of NIST-developed S-CAP content files.
- Provides mapping of security checks to CCE identifiers.
- Provides runtime notes – allowing auditors and security engineers to verify and validate assessment decisions.

Security Patch Checks & Vulnerability Assessment

- Automatically determines if computers have all required security patches.
- Performs vulnerability assessment of operating system and major applications.
- Automated update system keeps application and assessment content current.

Configuration and Security Remediation & Undo

- If discrepancies are discovered, Secutor Prime can automatically modify the configuration and security settings to bring systems into compliance.
- Secutor Prime can fix all problems or just those selected by the user.
- Perform remediation undo of individual rules or full system restore.

Standards-Based Assessment System

- Incorporates optimized XCCDF document parsing engine .
- Supports OVAL version 5.x as a definitions evaluator.
- Includes the first assessment engine to pass OVAL 5.0 certification testing.
- Supports the CPE, CCE, CVSS, and CVE standards.

Security Reporting & Data Export

- Includes HTML-based reports suitable for printing and drill-down.
- Exports CSV, OVAL thin and full results files, compressed or uncompressed.

Architecture & Supported Platforms

- Windows XP, Vista, 2003 Server, and 2000 - more as NIST releases content.
- Requires Java Run-time Environment 1.4x or greater (included).

ThreatGuard Secutor Compliance Automation Toolkit (S-Cat)

Overview

The Secutor Compliance Automation Toolkit (S-CAT) enables product vendors to easily add NIST’s Security Content Automation Protocol (SCAP) compatible compliance technology to their solutions. Over the years, ThreatGuard has earned a reputation for developing superb technology that embraces and enhances U.S. Government security standards. Our S-CAT modules allow organizations to implement these standards in days rather than the man-years required for custom development. The S-CAT modules are fast, lightweight and include all the power and efficiency you’ve come to expect from ThreatGuard. With ThreatGuard and S-CAT, implementing standard compliance solutions has never been so easy.

How does it help me?

S-CAT is a collection of libraries and executables that work together to form a comprehensive security compliance system. These development components can be added to third-party systems and accessed directly by calling the S-CAT API, scripted using the extensive command-line options, as a CGI binary, or through access to our SOA-ready agent. Developers can customize solutions by using only those components required to provide the desired functionality.

S-CAT Capabilities and Features:

Compliance Auditing, Exceptions, and Remediation

- The fastest assessment and remediation engines in the industry.
- Supports local exceptions-based policy deviations.
- Extremely simple installation, including support for unattended installs such as logon scripts or SMS jobs.
- Based on first assessment engine to pass OVAL 5.0 certification.
- Agent can be accessed directly via SOAP-RPC model or more efficiently via local broker library (Available as: .Net assembly, CLI, CGI, Java jar).
- Standalone assessment library can easily be integrated with existing environments and system agents via APIs or as a native executable.
- Supports all platforms for which there are OVAL or XCCDF content, including full FISMA checks for the OMB mandated platforms.
- Integrated server support for multiple data store types: flat files, MSDE, Sybase, Oracle, MySQL, etc.
- Results available as standards-compliant reports or raw XML data sets.
- Includes a collection of pre-built products including HTML/DHTML reports, PDF reports, CSV and XML exporting.

Integration features

- SOA ready (supports SOAP-RPC).
- Supports agentless usage over the network for Windows, Linux, Solaris, HP-UX and other operating systems and device types.

Integration Environments

- .Net framework version 2.0 or greater or any Java Runtime Environment of at least version 1.5.

Product Code	Product Name	SIN	Retail Price	GSA Price
TBFF0001	ThreatGuard CVMS in any mode (License for 500 nodes)	132-3	$20,000	$15,000
TBTF0001	ThreatGuard CVMS Traveler in appliance mode only (unlimited scanning)	132-3	$50,000	$40,000
TBFFR001	ThreatGuard CVMS in any mode full annual renewal for 500 nodes	132-3	$5,000	$4,000
TRTFR001	ThreatGuard CVMS Traveler annual renewal fee for updates	132-3	$20,000	$15,000
TBSM0001	ThreatGuard Secutor Magnus with single client license	132-3	$40 per seat	$30 per seat
TBSM0002	ThreatGuard Secutor Magnus with single client license - 3 year license (10% discount)	132-3	$108 per seat	$81 per seat
TBSM0003	ThreatGuard Secutor Magnus with single client license (including phone and e-mail support) support	132-3	$50 per seat	$37 per seat
TBSM0004	ThreatGuard Secutor Magnus with single client license (including phone and e-mail support) - 3 year license (10% discount)	132-3	$135 per seat	$100 per seat
TBSM0005	ThreatGuard Secutor Magnus with single server license	132-3	$134 per seat	$100 per seat
TBSM0006	ThreatGuard Secutor Magnus with single server license - 3 year license (10% discount)	132-3	$362 per seat	$270 per seat
TBSM0007	ThreatGuard Secutor Magnus with single server license (including phone and e-mail support) support	132-3	$168 per seat	$125 per seat
TBSM0008	ThreatGuard Secutor Magnus with single server license (including phone and e-mail support) - 3 year license (10% discount)	132-3	$454 per seat	$338 per seat
TBSMR001	ThreatGuard Secutor Magnus server with client software annual renewal fee	132-3	$40 per seat	$30 per seat

Product Code	Product Name	SIN	Retail Price	GSA Price
TBSMR002	ThreatGuard Secutor Magnus server with client software (including phone and e-mail support) annual renewal fee	132-3	$50 per seat	$37 per seat
TGSMD001	ThreatGuard Secutor Magnus server with client software for desktops	132-3	$40 per seat	$30 per seat
TGSMS001	ThreatGuard Secutor Magnus server with client software for servers	132-3	$134 per server	$100 per server
TGSMR001	ThreatGuard Secutor Magnus server with client software annual renewal fee	132-3	30% of cost	20% of cost
TGSPS001	ThreatGuard Secutor Prime Standard (Annual Fee)	132-3	$2,700	$2,025
TGSPP001	ThreatGuard Secutor Prime Professional (Annual Fee)	132.3	$3,300	$2,475
TGSC001	ThreatGuard S-CAT (Based on User numbers. Minimum Fee $25,000)	132-3	Based on Use	Based on Use
TGSC002	ThreatGuard S-CAT Annual Renewal Fee	132-3	30% of cost	20% of cost

NetIQ DESCRIPTIVE INFORMATION

NetIQ Aegis Base Server

NetIQ Aegis is a software platform that models, automates, measures, and improves run books and ITIL®-based processes bringing control and automation to IT Operations and Security. Key features include:

- Integration, User and Knowledge Administration
- Drag-and-Drop Workflow Designer
- Scheduler
- Enterprise-Ready Process Management
- Embedded Correlation Engine
- Real-time Process Monitoring
- Continuous Improvement Reporting

NetIQ Aegis Managed Object for Servers

Licensed per server, Aegis gives you the ability to immediately automate mundane, repetitive aspects of IT operations while providing the foundation for aggregating and consolidating those tasks to achieve the larger goal of automating processes that span functional disciplines such as those defined by ITIL. Through automation, Aegis acts like a force multiplier, offloading routine or mundane tasks so operators and administrators become more productive with less risk of human error and the associated re-work. Aegis enables rapid translation of existing processes into automated workflows without needing to rip and replace tools already in use. Aegis includes a built-in correlation engine that reduces the number of events from multiple sources and re-prioritizes events based on service impact, reducing the cost of incident and problem management. Aegis supplies built in performance metrics that help you benchmark performance, identify bottlenecks, streamline operations, and apply continuous improvement methods. Aegis gives you greater control of daily activities for more consistent service delivery and automated compliance with IT policies, with less policy training overhead and less burdensome documentation.

NetIQ Aegis Managed Object for Workstations

Licensed per workstations, through automation, Aegis acts like a force multiplier, offloading routine or mundane tasks so operators and administrators become more productive with less risk of human error and the associated re-work. Aegis enables rapid translation of existing processes into automated workflows without needing to rip and replace tools already in use. Aegis includes a built-in correlation engine that reduces the number of events from multiple sources and re-prioritizes events based on service impact, reducing the cost of incident and problem management.

Aegis supplies built in performance metrics that help you benchmark performance, identify bottlenecks, streamline operations, and apply continuous improvement methods.

Aegis gives you greater control of daily activities for more consistent service delivery and automated compliance with IT policies, with less policy training overhead and less burdensome documentation

NetIQ Secure Configuration Manager/SCAP Combo for Servers

SCAP Combo for Servers enables you to quickly identify FISMA and FDCC compliance across your enterprise. It provides a mechanism to easily establish a baseline for current system configuration; tracks and controls changes as they occur; comes with extensive out-of-the-box security and compliance knowledge and templates to reduce cost and accelerate compliance efforts; and helps you establish and clearly demonstrate successful compliance with policies and regulations.

NetIQ Secure Configuration Manager/SCAP Combo for Workstations

SCAP Combo for Workstations is agent technology that allows you to monitor systems for compliance, remediate setting on systems, and to schedule jobs and reports gathering tasks.

NetIQ Secure Configuration Manager Console

Configuration Manager Console enables you to install deploy agents, create reports for regulatory compliance for instance FDCC, FISMA. Create users to use Secure Configuration Manager and create policy to run against your environment.

Product Code	Product Name	SIN	Retail Price	GSA Price
TGNQ001	NetIQ Base Server	132-3	$25,000	$14,250
TGNQ001M	NetIQ Base Server – Maintenance	132-3	$4,500	$3,150
TGNQ002	NetIQ Aegis Managed Object for Servers	132-3	$300	$171
TGNQ002M	NetIQ Aegis Managed Object for Servers – Maintenance	132-3	$54.00	$37.80
TGNQ003	NetIQ Aegis Managed Object for Workstations	132-3	$30.00	$17.10
TGNQ003M	NetIQ Aegis Managed Object for Workstations – Maintenance	132.3	$5.00	$3.78
TGNQ004	NetIQ Secure Configuration Manager – SCAP Combo for Servers	132-3	$1,289	$734.73
TGNQ004M	NetIQ Secure Configuration Manager – SCAP Combo for Servers – Maintenance	132-3	$232.02	$162.41
TGNQ005	NetIQ Secure Configuration Manager – SCAP Combo for Workstations	132-3	$69.00	$39.33
TGNQ005M	NetIQ Secure Configuration Manager – SCAP Combo for Workstations – Maintenance	132-3	$12.42	$8.69
TGNQ006	NetIQ Secure Configuration Manager Console – (Unlimited Users) – Required	132-3	$2,500	$1,425
TGNQ006M	NetIQ Secure Configuration Manager Console – Maintenance	132-3	$450	$315